House Select Intelligence Committee Holds Hearing on Disclosure of National Security Agency Surveillance Programs

June 18, 2013

ROGERS:

The committee will come to order.

General Alexander, Deputy Attorney General Cole, Chris Inglis, Deputy Director Joyce and Mr. Litt, thank you for appearing before us today, especially on short notice.

The ranking member and I believe it is important to hold an open hearing today, and we don't do a tremendous amount of those, to provide this House and the public with an opportunity to hear directly from you how the government is using the legal authorities that Congress has provided to the executive branch since the terrorist attacks of September 11th, 2001.

I'd also like to recognize the hard work of the men and women of the NSA and the rest of the intelligence community who work day in and day out to disrupt threats to our national security. People at the NSA in particular have heard a constant public drumbeat about a laundry list of nefarious things they are alleged to be doing to spy on Americans -- all of them wrong. The misperceptions have been great, yet they keep their heads down and keep working every day to keep us safe.

ROGERS:

And, General Alexander, please convey our thanks to your team for continuing every day, despite much misinformation about the quality of their work. And thank them for all of us for continuing to work to protect America.

I also want to take this moment to thank General Alexander who has been extended as national security adviser in one way or another three different times. That's a patriot.

This is a very difficult job at a very difficult time in our history. And for the general to accept those extensions of his military service to protect this nation, I think with all of the -- the, again, the misinformation out there, I want to thank you for that.

Thank you for your patriotism. Thank you for continuing to serve to protect the United States, again. And you have that great burden of knowing lots of classified information you cannot talk publicly about. I want you to know, thank you on behalf of America for your service to your country.

The committee has been extensively briefed on these efforts over a regular basis as a part of our ongoing oversight responsibility over the 16 elements of the intelligence community and the national intelligence program.

In order to fully understand the intelligence collection programs most of these briefings and hearings have taken place in classified settings. Nonetheless, the collection efforts under the business records provision in Section 702 of the Foreign Intelligence Surveillance Act are legal, court-approved and

subject to an extensive oversight regime.

I look forward from hearing from all of the witnesses about the extensive protections and oversight in place for these programs.

General Alexander, we look forward to hearing what you're able to discuss in an open forum about how the data that you have -- you obtain from providers under court order, especially under the business records provision, is used.

And Deputy Attorney General Cole, we look forward to hearing more about the legal authorities themselves and the state of law on what privacy protections Americans have in these business records.

One of the frustrating parts about being a member of this committee, and really challenge, is sitting at the intersection of classified intelligence programs and transparent democracy as representatives of the American people.

The public trusts the government to protect the country from another 9/11-type attack, but that trust can start to wane when they are faced with inaccuracies, half truths and outright lies about the way the intelligence programs are being run.

One of the more damaging aspects of selectively leaking incomplete information is that it paints an inaccurate picture and fosters distrust in our government.

This is particularly so when those of us who have taken the oath to protect information that can damage the national security if released cannot publicly provide clarifying information because it remains classified.

It is at times like these where our enemies with -- our enemies within become almost as damaging as our enemies on the outside.

It is critically important to protect sources and methods so we aren't giving the enemy our play book.

It's also important, however, to be able to talk about how these programs help protect us so they can continue to be reauthorized. And then we highlight the protections and oversight of which these programs operate under.

General Alexander, you and I have talked over the last week, about the need to -- to be able to publicly elaborate on the success stories these authorities have contributed to without jeopardizing ongoing operations. I know you'll have the opportunity to talk about several of those today.

I place the utmost value in protecting sources and methods. And that's why you've been, I think, so diligent in making sure that anything that's disclosed comports with the need to protect sources and methods. So that, again, we don't make it easier for the bad guys overseas, terrorists in this case, to do harm to United States citizens, and I respect that.

I also recognize that when we are forced into the position of having so publicly discussed intelligence programs due to irresponsible criminal behavior that we also have to be careful to balance the need for secrecy while educating the public.

I think you have struck the right balance between protecting sources and methods and maintaining the public's trust by providing more examples of how these authorities have helped disrupt terrorist plots

and connections. I appreciate your efforts in this regard.

For these authorities to continue, they must continue to be available. Without them, I fear we will return to the position where we were prior to the attacks of September 11th, 2001. And that would be unacceptable for all of us.

I hope today's hearing will help answer questions that have arisen as a result of the fragmentary and distorted illegal disclosures over the past several days.

Before recognizing General Alexander for his opening statement, I turn the floor over to the ranking member for any opening statement he'd like to make.

RUPPERSBERGER:

Well, I agree with really a lot of what the chairman said.

General Alexander, Chris Inglis, you know, your leadership in NSA has been outstanding. And I just want to acknowledge the people who work at NSA every day. NSA is in my district. I have an occasion to communicate, and a lot of the people who go to work to protect our country, who work hard every day, are concerned that the public think they're doing something wrong. And that's not the case at all.

And the most important thing we can do here today is let the public know the true facts. I know that Chairman Rogers and I and other members have asked you to help declassify what we can, that will not hurt our security, so the public can understand that this important (sic) is legal, why we're doing this program and how it protects us.

We're here today because of the brazen disclosure of critical classified information that keeps our country safe. This widespread leak by a 29-year-old American systems administrator put our country and our allies in danger by giving the terrorists a really good look at the play book that we use to protect our country. The terrorists now know many of our sources and methods.

There's been a lot in the media about this situation. Some right. A lot wrong. We're holding this open hearing today so we can set the record straight and the American people can hear directly from the intelligence community as to what is allowed and what is not under the law. We need to educate members of Congress also, with the public.

To be clear, the National Security Agency is prohibited from listening in on phone calls of Americans without proper, court- approved legal authorities.

We live in a country of laws. These laws are strictly followed and layered with oversight from three branches of government, including the executive branch, the courts and Congress.

Immediately after 9/11, we learned that a group of terrorists were living in the United States actively plotting to kill Americans on our own soil. But we didn't have the proper authorities in place to stop them before they could kill almost 3,000 innocent people.

Good intelligence is clearly the best defense against terrorism. There are two main authorities that have been highlighted in the press, the business records provision that allows the government to legally collect what is called metadata, simply the phone number and length of call. No content, no conversations. This authority allows our counterterrorism and the law enforcement officials to close the gap on foreign and

domestic terrorist activities. It enables our intelligence community to discover whether foreign terrorists have been in contact with people in the U.S. who may be planning a terrorist attack on U.S. soil.

The second authority is known as Section 702 of the FISA Amendment Act. It allows the government to collect the content of e- mail and phone calls of foreigners -- not Americans -- located outside the United States. This allows the government to get information about terrorists, cyber-threats, weapons of mass destruction and nuclear weapons proliferation that threaten America.

This authority prohibits the targeting of American citizens or U.S. permanent residents without a court order, no matter where they are located.

Both of these authorities are legal. Congress approved and reauthorized both of them over the last two years. In fact, these authorities have been instrumental in helping prevent dozens of terrorist attacks, many on U.S. soil.

But the fact still remains that we must figure out how this could have happened. How was this 29-year-old systems administrator able to access such highly classified information and about such sensitive matters? And how was he able to download it and remove it from his workplace undetected?

We need to change our systems and practices, and employ the latest in technology that would alert superiors when a worker tries to download and remove this type of information. We need to seal this crack in the system.

And to repeat something incredibly important: The NSA is prohibited from listening to phone calls or reading e-mails of Americans without a court order. Period. End of story.

Look forward your testimony.

ROGERS:

Again, thank you very much.

Thanks, Dutch, for that.

General Alexander, the floor is yours.

ALEXANDER:

Chairman, Ranking Member, thank you for the kind words. I will tell you it is a privilege and honor to serve as the director of the National Security Agency and the commander of the U.S. Cyber Command.

As you noted, we have extraordinary people doing great work to protect this country and to protect our civil liberties and privacy.

Over the past few weeks, unauthorized disclosures of classified information have resulted in considerable debate in the press about these two programs.

The debate had been fueled, as you noted, by incomplete and inaccurate information, with little context provided on the purpose of these programs, their value to our national security and that of our allies, and the protections that are in place to preserve our privacy and civil liberties.

Today, we will provide additional detail and context on these two programs to help inform that debate.

These programs were approved by the administration, Congress and the courts. From my perspective, a sound legal process that we all work together as a government to protect our nation and our civil

liberties and privacy.

ALEXANDER:

Ironically, the documents that have been released so far show the rigorous oversight and compliance our government uses to balance security with civil liberties and privacy.

Let me start by saying that I would much rather be here today debating this point than trying to explain how we failed to prevent another 9/11. It is a testament to the ongoing team work of the Central Intelligence Agency, the Federal Bureau of Investigation, and the National Security Agency, working with our allies and industry partners, that we have been able to connect the dots and prevent more terrorist attacks.

The events of September 11, 2001 occurred, in part, because of a failure on the part of our government to connect those dots. Some of those dots were in the United States. The intelligence community was not able to connect those domestic dots, phone calls between operatives and the U.S. and Al Qaida terrorist overseas. Following the 9/11 commission, which investigated the intelligence community's failure to detect 9/11, Congress passed the PATRIOT Act.

Section 215 of that act, as it has been interpreted and implied, helps the government close that gap by enabling the detection of telephone contact between terrorists overseas and operatives within the United States. As Director Mueller emphasized last week during his testimony to the -- to the Judiciary Committee, if we had had Section 215 in place prior to 9/11, we may have known that the 9/11 hijacker Mihdhar was located in San Diego and communicating with a known Al Qaida safe house in Yemen.

In recent years, these programs, together with other intelligence, have protected the U.S. and our allies from terrorist threats across the globe to include helping prevent the terrorist -- the potential terrorist events over 50 times since 9/11. We will actually bring forward to the committee tomorrow documents that the interagency has agreed on, that in a classified setting, gives every one of those cases for your review. We'll add two more today publicly we'll discuss. But as the chairman noted, if we give all of those out, we give all the secrets of how we're tracking down the terrorist as a community. And we can't do that. Too much is at risk for us and for our allies. I'll go into greater detail as we go through this testimony this morning.

I believe we have achieved the security and relative safety in a way that does not compromise the privacy and civil liberties of our citizens. We would like to make three fundamental points. First, these programs are critical to the intelligence community's ability to protect our nation and our allies' security. They assist the intelligence community efforts to connect the dots.

Second, these programs are limited, focused, and subject to rigorous oversight. They have distinct purposes in oversight mechanisms. We have rigorous train programs for our analysts and their supervisors to understand their responsibilities regarding compliance.

Third, the disciplined operation of these programs protects the privacy and civil liberties of the American people. We will provide important details about each of those. First, I'd -- I'd ask the Deputy Attorney General Jim Cole to discuss the overarching framework of our authority.

Sir.

COLE:

Thank you -- thank you, General.

Mr. Chairman, Mr. Ranking Member, members of the committee, as General Alexander said, and -- and as the chairman and ranking member have said, all of us in the national security area are constantly trying to balance protecting public safety with protecting people's privacy and civil liberties in this government. And it's a constant job at balancing this.

We think we've done this in these instances. There are statutes that are passed by Congress. This -- this is not a program that's off the books, that's been hidden away. This is part of what government puts together and discusses. Statutes are passed. It is overseen by three branches of our government, the Legislature, the Judiciary, and the Executive Branch. The process of oversight occurs before, during, and after the processes that we're talking about today.

And I want to talk a little bit how that works, what the legal framework is, and what some of the protections are that are put into it. First of all, what we have seen published in the newspaper concerning 215 -- this is the business records provisions of the PATRIOT Act that also modify FISA.

You've seen one order in the newspaper that's a couple of pages long that just says under that order, we're allowed to acquire metadata, telephone records. That's one of two orders. It's the smallest of the two orders. And the other order, which has not been published, goes into, in great detail; what we can do with that metadata; how we can access it; how we can look through it; what we can do with it, once we have looked through it; and what the conditions are that are placed on us to make sure that we protect privacy and civil liberties; and, at the same time, protect public safety.

Let me go through a few of the features of this. First of all, it's metadata. These are phone records. These -- this is just like what you would get in your own phone bill. It is the number that was dialed from, the number that was dialed to, the date and the length of time. That's all we get under 215. We do not get the identity of any of the parties to this phone call. We don't get any cell site or location information as to where any of these phones were located. And, most importantly, and you're probably going to hear this about 100 times today, we don't get any content under this. We don't listen in on anybody's calls under this program at all.

This is under, as I said, section 215 of the PATRIOT Act. This has been debated and up for reauthorization, and reauthorized twice by the United States Congress since its inception in 2006 and in 2011. Now, in order -- the way it works is, the -- there is an application that is made by the FBI under the statute to the FISA court. We call it the FISC. They ask for and receive permission under the FISC under this to get records that are relevant to a national security investigation. And they must demonstrate to the FISC that it will be operated under the guidelines that are set forth by the attorney general under executive order 12333. This is what covers intelligence gathering in the federal government.

It is limited to tangible objects. Now, what does that mean? These are like records, like the metadata, the phone records I've been describing. But it is quite explicitly limited to things that you could get with a grand jury subpoena, those kinds of records. Now, it's important to know prosecutors issue grand jury subpoenas all the time and do not need any involvement of a court or anybody else, really, to do so.

Under this program, we need to get permission from the court to issue this ahead of time. So there is court involvement with the issuance of these orders, which is different from a grand jury subpoena. But

the type of records, just documents, business records, things like that, are limited to those same types of records that we could get through a grand jury subpoena.

Now, the orders that we get last 90 days. So we have to re-up and renew these orders every 90 days in order to do this. Now, there are strict controls over what we can do under the order. And, again, that's the bigger, thicker order that hasn't been published. There's restrictions on who can access it in this order. It is stored in repositories at NSA that can only be accessed by a limited number of people. And the people who are allowed to access it have to have special and rigorous training about the standards under which that they can access it.

In order to access it, there needs to be a finding that there is responsible suspicion that you can articulate, that you can put into words, that the person whose phone records you want to query is involved with some sort of terrorist organizations. And they are defined. It's not everyone. They are limited in the statute. So there has to be independent evidence, aside from these phone records, that the person you're targeting is involved with a terrorist organization.

COLE:

If that person is a United States person, a citizen, or a lawful permanent resident, you have to have something more than just their own speeches, their own readings, their own First Amendment-type activity. You have to have additional evidence beyond that that indicates that there is reasonable, articulable suspicion that these people are associated with specific terrorist organizations.

Now, one of the things to keep in mind is under the law, the Fourth Amendment does not apply to these records. There was a case quite a number of years ago by the Supreme Court that indicated that toll records, phone records like this, that don't include any content, are not covered by the Fourth Amendment because people don't have a reasonable expectation of privacy in who they called and when they called. That's something you show to the phone company. That's something you show to many, many people within the phone company on a regular basis.

Once those records are accessed under this process and reasonable articulable suspicion is found, that's found by specially trained people. It is reviewed by their supervisors. It is documented in writing ahead of time so that somebody can take a look at it. Any of the accessing that is done is done in an auditable fashion. There is a trail of it. So both the decision and the facts that support the accessing and the query is documented. The amount that was done, what was done -- all of that is documented and reviewed and audited on a fairly regular basis.

There are also minimization procedures that are put into place so that any of the information that is acquired has to be minimized. It has to be limited and its use is strictly limited. And all that is set out in the terms of the court order. And if any U.S. persons are involved, there are particular restrictions on how any information concerning a U.S. person can be used in this.

Now, there is extensive oversight and compliance that is done with these records and with this process. Every now and then, there may be a mistake -- a wrong phone number is hid or a person who shouldn't have been targeted gets targeted because there is a mistake in the phone record, something like that.

Each of those compliance incidents, if and when they occur, have to be reported to the FISA court immediately. And let me tell you, the FISA court pushes back on this. They want to find out why did this happen, what were the procedures and the mechanisms that allowed it to happen, and what have

you done to fix it. So whenever we have a compliance incident, we report it to the court immediately and we report it to Congress. We report it to the Intelligence Committees of both houses and the Judiciary Committees of both houses.

We also provide the Intelligence and Judiciary Committees with any significant interpretations that the court makes of the 215 statute. If they make a ruling that is significant or issue an order that is significant in its interpretation, we provide those, as well as the applications we made for those orders, to the Intelligence Committee and to the Judiciary Committee.

And every 30 days, we are filing with the FISC, with the court, a report that describes how we implement this program. It includes a discussion of how we're applying the reasonable, articulable suspicion standard. It talks about the number of approved queries that we made against this database, the number of instances that the query results and contain a U.S. person information that was shared outside of NSA. And all of this goes to the court.

At least once every 90 days and sometimes more frequently, the Department of Justice, the Office of the Director of National Intelligence, and the NSA meet to assess NSA's compliance with all of these requirements that are contained in the court order. Separately, the Department of Justice meets with the inspector general for the National Security Agency and assesses NSA's compliance on a regular basis.

Finally, there is by statute reporting of certain information that goes to Congress in semiannual reports that we make on top of the periodic reports we make if there's a compliance incident. And those include information about the data that was required and how we are performing under this statute.

So once again keeping in mind, all of this is done with three branches of government involved: oversight and initiation by the executive branch with review by multiple agencies; statutes that are passed by Congress, oversight by Congress; and then oversight by the court.

Now, the 702 statute under the FISA Amendments Act is different. Under this, we do get content, but there's a big difference. You are only allowed under 702 to target for this purpose non-U.S. persons who are located outside of the United States. So if you have a U.S. permanent resident who's in Madrid, Spain, we can't target them under 702. Or if you have a non-U.S. person who's in Cleveland, Ohio, we cannot target them under 702. In order to target a person, they have to be neither a citizen nor a permanent U.S. resident, and they need to be outside of the United States while we're targeting them.

Now, there's prohibitions in this statute. For example, you can't reverse-target somebody. This is where you target somebody who's out of the United States, but really your goal is to capture conversations with somebody who is inside the United States. So you're trying to do indirectly what you couldn't do directly. That is explicitly prohibited by this statute. And if there is ever any indication that it's being done, because again, we report the use that we make of this statute to the court and to the Congress, that is seen.

You also have to have a valid foreign intelligence purpose in order to do any of the targeting on this. So you have to make sure, as it was described, that it's being done for defined categories of weapons of mass destruction, foreign intelligence, things of that nature. These are all done pursuant to an application that is made by the attorney general and the director of national intelligence to the FISC. The FISC gives a certificate that allows this targeting to be done for a year period. It then has to be renewed at the end of that year in order for it to be re-upped.

Now, there's also there is a requirement that, again, there is reporting. You cannot under the terms of this statute have and collect any information on conversations that are wholly within the United States. So you're targeting someone outside the United States. If they make a call to inside the United States, that can be collected, but it's only because the target of that call outside the United States initiated that call and went there. If the calls are wholly within the United States, we cannot collect them.

If you're targeting a person who is outside of the United States and you find that they come into the United States, we have to stop the targeting right away. And if there's any lag and we find out that we collected information because we weren't aware that they were in the United States, we have to take that information, purge it from the systems, and not use it.

Now, there's a great deal of minimization procedures that are involved here, particularly concerning any of the acquisition of information that deals or comes from U.S. persons. As I said, only targeting people outside the United States who are not U.S. persons. But if we do acquire any information that relates to a U.S. person, under limited criteria only can we keep it.

If it has to do with foreign intelligence in that conversation or understanding foreign intelligence, or evidence of a crime or a threat of serious bodily injury, we can respond to that. Other than that, we have to get rid of it. We have to purge it, and we can't use it. If we inadvertently acquire any of it without meaning to, again, once that's discovered, we have to get rid of it. We have to purge it.

The targeting decisions that are done are, again, documented ahead of time, reviewed by a supervisor before they're ever allowed to take place in the beginning. The Department of Justice and the Office of the Director of National Intelligence conduct on-site reviews of each targeting that is done. They look at them to determine and go through the audit to determine that they were done properly. This is done at least every 60 days and many times done more frequently than that.

In addition, if there's any compliance issue, it is immediately reported to the FISC. The FISC, again, pushes back: How did this happen? What are the procedures? What are the mechanisms you're using to fix this? What have you done to remedy it? If you acquired information you should (sic) have, have you gotten rid of it as you're required? And in addition, we're providing Congress with all of that information if we have compliance problems.

We also report quarterly to the FISC concerning the compliance issues that have arisen during that quarter, on top of the immediate reports and what we've done to fix it and remedy the ones that we reported.

COLE:

We also to Congress under this program, the Department of Justice and the Office of the Director of National Intelligence provide a semiannual report to the FISC and to Congress assessing all of our compliance with the targeting and minimization procedures that are contained in the court order. We also provide a semi-annual report to the FISC and Congress concerning the implementation of the program, what we've done and what we've found. And we also provide to Congress, documents that contain again, how we're dealing with the minimization procedures, any significant legal interpretations that the FISC makes concerning these statutes, as well as the orders and the applications that would relate to that.

And on top of all of this, annually the inspector general for NSA does an assessment, which he provides

to Congress that reports on compliance, the number of disseminations under this program that relate to U.S. persons, the number of targets that were reasonably believed at the time to be outside the United States who were later determined to be in the United States, and when that was done. So in short, there is, from before, during and after the involvement of all three branches of the United States government, on a robust and fairly intimate way. I'd like to make one other observation, if I may, on this. We have tried to do this in as thorough, as protective, and as transparent a way as we possibly can, considering it is the gathering of intelligence information.

Countries and allies of ours all over the world collect intelligence. We all know this. And there have recently been studies about how transparent our system is in the United States, compared to many of our partners, many in the E.U. Countries like France, the U.K., Germany, who we work with regularly. And a report that was just recently issued in May of this year found that the FISA Amendments Act, the statute that we're talking about here, and I will quote, "Imposes at least at much, if not more, due process and oversight on foreign intelligence surveillance than other countries." And this includes E.U. countries. And it says under this, the U.S. is more transparent about its procedures, requires more due process protections in its investigations that involve national security, terrorism and foreign intelligence.

The balance is always one we seek to strive to -- to achieve. But I think as I've laid out to you, we have done everything we can to achieve it. And I think part of the proof of what we've done is this report that came out just last month, indicating our system is as good, and frankly better, than all of our allies and liaison partners. Thank you Mr. Chairman.

ALEXANDER:

Mr. Chairman, I will now switch to the value of the program, and talk about some statistics that we're putting together. As we stated, these programs are immensely valuable for protecting our nation, and security the security of our allies. In recent years, the information gathered from these programs provided the U.S. government with critical leads to help prevent over 50 potential terrorist events in more than 20 countries around the world. FAA 702 contributed in over 90 percent of these cases. At least 10 of these events included homeland-based threats. In the vast majority, business records, FISA reporting contributed as well. I would also point out that it is a great partnership with the Department of Homeland Security in those with a domestic nexus.

But the real lead for domestic events is the Federal Bureau of Investigation. It has been our honor and privilege to work with Director Mueller, and Deputy Directory Joyce who -- I'll turn it now over to Sean?

JOYCE:

Thank you General. Thank you chairman and ranking member, and members of the committee for the opportunity to be here today. NSA and the FBI have a unique relationship, and one that has been invaluable since 9/11. And I just want to highlight a couple of the instances. In the fall of 2009, NSA using 702 authority intercepted an e-mail from a terrorist located in Pakistan. That individual was talking with an individual located inside the United States, talking about perfecting a recipe for explosives. Through legal process, that individual was identified as Najibullah Zazi. He was located in Denver, Colorado.

The FBI followed him to New York City. Later we executed search warrants with the New York Joint

Terrorism Task Force and NYPD and found bomb-making components in backpacks. Zazi later confessed to a plot to bomb the New York subway system with backpacks. Also working with FISA business records, the NSA was able to provide a previously unknown number of one of the co-conspirators -- co-conspirators, Adis Medunjanin. This was the first core Al Qaida plot since 9/11 directed from Pakistan. Another example, NSA utilizing 702 authority was monitoring a known extremist in Yemen. This individual was in contact with an individual in the United States named Khalid Ouazzani. Ouazzani and other individuals that we identified through a FISA that the FBI applied for through the FISC were able to detect a nascent plotting to bomb the New York Stock Exchange.

Ouazzani had been providing information and support to this plot. The FBI disrupted and arrested these individuals. Also David Headley, a U.S. citizen living in Chicago. The FBI received intelligence regarding his possible involvement in the 2008 Mumbai attacks responsible for the killing of over 160 people. Also, NSA through 702 coverage of an Al Qaida affiliated terrorist found that Headley was working on a plot to bomb a Danish newspaper office that had published the cartoon depictions of the Prophet Mohammed. In fact, Headley later confessed to personally conducting surveillance of the Danish newspaper office. He, and his co-conspirators were convicted of this plot.

Lastly, the FBI had opened an investigation shortly after 9/11. We did not have enough information, nor did we find links to terrorism and then we shortly thereafter closed the investigation. However, the NSA using the business record FISA tipped us off that this individual had indirect contacts with a known terrorist overseas. We were able to reopen this investigation, identify additional individuals through a legal process, and were able to disrupt this terrorist activity. Thank you. Back to you, General?

ALEXANDER:

So that's four cases total that we've put out publicly. What we're in the process of doing with the inter-agency is looking at over 50 cases that were classified, and will remain classified, that will be provided to both of the Intel Committees of the Senate and the House, to all of you. Those 50 cases right now have been looked at by the FBI, CIA and other partners within the community, and the National Counterterrorism Center is validating all of the points so that you know that what we've put in there is exactly right. I believe the numbers from those cases is something that we can publicly reveal, and all publicly talk about.

What we are concerned, as the chairman said, is to going into more detail on how we stopped some of these cases, as we are concerned it will give our adversaries a way to work around those, and attack us, or our allies. And that would be unacceptable. I have concerns that the intentional and irresponsible release of classified information about these programs will have a long, and irreversible impact on our nation's security, and that of our allies. This is significant. I want to emphasize that the Foreign Intelligence is the best -- the Foreign Intelligence Program that we're talking about, is the best counterterrorism tools that we have to go after these guys.

We can't lose those capabilities. One of the issues that has repeatedly come up, well how do you then protect civil liberties and privacy? Where is the oversight? What are you doing on that? We have the deputy director of the National Security Agency, Chris Inglis, will now talk about that and give you some specifics about what we do, and how we do it with these programs.

INGLIS:

Thank you, General Alexander.

Chairman, Ranking Member, members of the committee, I'm pleased to be able to briefly describe the two programs as used by the National Security Agency with a specific focus on the internal controls and the oversight provided. Now first to remind these two complimentary, but distinct programs are focused on foreign intelligence. That's NSA's charge. The first program executed under Section 215 of the Patriot Act authorizes he collection of telephone metadata only. As you've heard before, the metadata is only the telephone numbers, and contact, the time and date of the call, and the duration of that call.

INGLIS:

This authority does not, therefore, allow the government to listen in on anyone's telephone calls, even that of a terrorist. The information acquired under the court order from the telecommunications providers does not contain the content of any communications, what you are saying during the course of the conversation, the identities of the people who are talking, or any cell phone locational information. As you also know this program was specifically developed to allow the U.S. government to detect communications between terrorists operating outside the U.S., who are themselves communicating with potential operatives inside the U.S., a gap highlighted by the attacks of 9/11.

The controls on the use of this data at NSA are specific, rigorous, and designed to ensure focus on counter-terrorism. To that end, the metadata acquired and stored under this program may be queried only when there is a reasonable suspicion based on specific and documented facts that an identifier, like a telephone number, is associated with specific foreign terrorist organizations.

This determination is formally referred to as the "reasonable articulable suspicion standard." During all 2012, the 12 months of 2012, we at NSA approved fewer than 300 unique numbers, which were then used to initiate a query of this data set.

The second program, authorized under Section 702 of the Foreign Intelligence Surveillance Act, authorizes targeting only for communications of foreigners who are themselves not within the United States for foreign intelligence purposes, with the compelled assistance of an electronic communications service provider.

As I noted earlier, NSA being a foreign intelligence agency, foreign intelligence for us is information related to the capabilities, intentions, or activities of foreign governments, foreign organizations, foreign persons, or international terrorists. Let me be very clear. Section 702 cannot be and is not used to intentionally target any U.S. citizen or any U.S. person, any person known to be in the United States, a person outside the United States if the purpose is to acquire information from a person inside the United States. We may not do any of those things using this authority.

The program is also key in our counter-terrorism efforts, as you've heard. More than 90 percent of the information used to support the 50 disruptions mentioned earlier was gained from this particular authority. Again, if you want to target the content of a U.S. person anywhere in the world, you cannot use this authority. You must get a specific court warrant.

I'd like to now describe in further details some of the rigorous oversight for each of these programs. First, for the Section 215 program, also referred to as business records FISA, controls and (ph) determine how we manage and use the data are explicitly defined and formally approved by the Foreign

Intelligence Surveillance Court.

First, the metadata segregated from other data sets held by NSA and all queries against the data base are documented and audited. As defined in the orders of the court, only 20 analysts at NSA and their two managers, for a total of 22 people, are authorized to approve numbers that may be used to query this database. All of those individuals must be trained in the specific procedures and standards that pertain to the determination of what is meant by reasonable, articulable suspicion.

Every 30 days, NSA reports to the court the number of queries and disseminations made during that period. Every 90 days, the Department of Justice samples all queries made across the period and explicitly reviews the basis for every U.S. person, or every U.S. identity query made. Again, we do not know the names of the individuals of the queries we might make.

In addition, only seven senior officials at NSA may authorize the dissemination of any information we believe that might be attributable to a U.S. person. Again, we would not know the name. It would only be the telephone number. And that dissemination in this program would only be made to the Federal Bureau of Investigation at determining that the information is related to and necessary to understand a counter-terrorism initiative.

The Foreign Intelligence Surveillance court reviews the program every 90 days. The data that we hold must be destroyed within five years of its acquisition. NSA and the Department of Justice briefed oversight committees on the employment of the program. We provide written notification of all significant developments within the program. The Department of Justice provides oversight committees with all significant foreign intelligence surveillance courts' opinions regarding the program.

Turning my attention to the 702 program, the Foreign Intelligence Surveillance Court annually reviews certification, which are required by law, that are jointly submitted by the attorney general and the director of national intelligence. These certifications define the categories of foreign actors that may be appropriately targeted and, by law, must include specific targeting and minimization procedures that the attorney general and the court both agree are consistent with the law and the Fourth Amendment of the Constitution. These procedures require that a communication of or concerning a U.S. person must be promptly destroyed after it's identified, either as clearly not relevant to the authorized purpose, or as not containing evidence of a crime.

The statute further requires a number of reports to be provided to both the court and the oversight committees. A semi-annual assessment by the Department of Justice and the Office of the Director of National Intelligence, regard in (ph) compliance with the targeting and minimization procedures an annual I.G. assessment that reports compliance with procedural requirements laid out within the order -- the number of disseminations that may refer to U.S. persons, the number of targets later found to be in the United States, and whether the communications of such targets were ever reviewed.

An annual director of NSA report is also required to describe the compliance efforts taken by NSA and address the number of U.S. person identities disseminated in NSA reporting. Finally, Foreign Intelligence Surveillance Court procedures require NSA to inform the court of any novel issues of law or technology relevant to an authorized activity and any non-compliance to include the Executive Branch's plan for remedying that same event. In addition to the procedures I've just described, the Department of Justice conducts on- site reviews at NSA to sample NSA's 702 targeting and tasking

decisions every 60 days.

And, finally, I would conclude with my section to say that in July of 2012, the Senate Select Committee on Intelligence, in a report reviewing the progress over the four years of the law's life at that point in time, said that across the four-year history of the program, the committee had not identified a single willful effort by the Executive Branch to violate the law.

ALEXANDER:

So to wrap up, Chairman, first I'd like to just hit on -- when we say seven officials, that's seven positions that -- at NSA can disseminate U.S. persons data. Today, there are 10 people in those positions. One of those is our -- SIGINT operations officer. Every one of those have to be -- credentialed. Chris and I are two of those officials.

I do want to hit a couple of key points. First, with our industry partners, under the 702 program, the U.S. government does not unilaterally obtain information from the servers of U.S. companies. Rather, the U.S. companies are compelled to provide these records by U.S. law, using methods that are in strict compliance with that law.

Further, as the deputy attorney general noted, virtually all countries have lawful intercept programs under which they compel communication providers to share data about individuals they believe represent a threat to their societies. Communication providers are required to comply with those programs in the countries in which they operate. The United States is not unique in this capability.

The U.S., however, operates its program under the strict oversight and compliance regime that was noted above with careful oversights by the courts, Congress, and the administration. In practice, U.S. companies have put energy and focus and commitment into consistently protecting the privacy of their customers around the world, while meeting their obligations under the laws of U.S. and other countries in which they operate. And I believe they take those seriously.

Our third and final point, as Americans, we value our privacy and our liberty -- our civil liberties. Americans -- as Americans, we also value our security and our safety. In the 12 years since the attacks on September 11th, we have lived in relative safety and security as a nation. That security is a direct result of the intelligence community's quiet efforts to better connect the dots and learn from the mistakes that permitted those attacks to occur on 9/11.

In those 12 years, we have thought long and hard about oversight and compliance and how we minimize the impact on our fellow citizens' privacy. We have created and implemented and continue to monitor -- monitor a comprehensive mission compliance program inside NSA. This program, which was developed based on industry best practices and compliance works to keep operations and technology aligned with NSA's externally approved procedures.

Outside of NSA, the officer of the -- the Office of the Director of National Intelligence, Department of Justice, and the Foreign Intelligence Surveillance Court provide robust oversight as well as this committee. I do believe we have that balance right.

In summary, these programs are critical to the intelligence community's ability to protect our nation and our allies' security. They assist the intelligence community's efforts to connect the dot. Second, these programs are limited, focused, and subject to rigorous oversight. They have distinct purposes and

oversight mechanisms. Third, the disciplined operation of these programs protects the privacy and civil liberties of the American people.

As you noted, Chairman, the people of NSA take these responsibilities to heart. They protect our nation and our allies as part of a bigger team. And they protect our civil liberties and privacy. It has been an honor and privilege to lead these great Americans. I think Bob Litt has a couple of comments to make, and then we'll turn it back to you, Chairman.

LITT:

Yes, Mr. Chairman, Mr. Ranking Member, members of the committee, I just want to speak very briefly and address a couple of additional misconceptions that the public has been fed about some of these programs.

The first is that collection under Section 702 of the FISA Amendments Act is somehow a loosening of traditional standards because it doesn't require individualized warrants. And, in fact, exactly the opposite is the case. The kind of collection that is done under Section 702, which is collecting foreign intelligence information for foreigners outside of the United States historically was done by the executive branch under its own authority without any kind of supervision whatsoever.

And as a result of the FISA Amendments Act, this has now been brought under a judicial process with the kind of restrictions and limitations that have been described by the other witnesses here. So, in fact, this is a tightening of standards from what they were before.

The second misconception is that the FISA court is a rubber stamp for the executive branch. And people point to the fact that the FISA court ultimately approves almost every application that the government submits to it.

But this does not recognize the actual process that we go through with the FISA court. The FISA court is judges, federal district judges appointed from around the country who take this on in addition to their other burdens. They're all widely respected and experienced judges. And they have a full-time professional staff that works only on FISA matters.

When we prepare an application for -- for a FISA, whether it's under one of these programs or a traditional FISA, we first submit to the court what's called a "read copy," which the court staff will review and comment on.

And if -- and they will almost invariably come back with questions, concerns, problems that they see. And there is an iterative process back and forth between the government and the FISA court to take care of those concerns so that at the end of the day, we're confident that we're presenting something that the FISA court will approve. That is hardly a rubber stamp. It's rather extensive and serious judicial oversight of this process.

The third point, the third misconception that I want to make is that the process we have here is one that simply relies on trust for individual analysts or individual people at NSA to obey the rules.

And I just -- I -- I won't go into detail as to the oversight, because I think it's been adequately described by the others. But the point is, there is a multilayered level of oversight, first within NSA, then involving my agency, the Office of the Director of National Intelligence and the Department of Justice and ultimately involving the FISA court and the Congress to ensure that these rules are complied with.

And the last point that I'd -- the last misconception I want to address is that this information shouldn't have been classified and it was classified only to -- to conceal it from the American people and that the leaks of this information are not damaging.

And, Mr. Chairman and Mr. Ranking Member, you both made this point. These are, as General Alexander said, extremely important collection programs to protect us not only from terrorists, but from other threats to our national security, a wide variety.

And they have produced a huge amount of valuable intelligence over the years. We are now faced with a situation that because this information has been made public, we run the risk of losing these collection capabilities. We're not gonna know for many months whether these leaks in fact have caused us to lose these capabilities. But if -- if they -- if they do have that effect, there is no doubt that they will cause our national security to be affected.

Thank you, Mr. Chairman.

ROGERS:

Thank you all, very much. I appreciate that. I just have a couple of quick questions. I know members have lots of questions here and I want to get to them.

Mr. Inglis, just for the record, you -- can you describe quickly your civilian role as the deputy? You serve as that role in a civilian capacity. Is that correct?

INGLIS:

Yes, sir. Across the history of NSA, there has always been a senior serving military officer, that's the director of the National Security Agency, and at the same time a senior serving civilian authority, and that would be the deputy director, and that's my role.

ROGERS:

All right, and -- but you have also had military service. Is that correct?

INGLIS:

Sir, I did. I served for a period of 13 years on active duty in the United States Air Force, and then transitioned to the National Security Agency.

ROGERS:

So you rose to the rank of -- of?

INGLIS:

I was brigadier general in the Air National Guard. As in all things, it's complicated.

(CROSSTALK)

ROGERS:

Yeah. But I just wanted to get on the record that you do have -- you have military service as well as your civilian service.

(CROSSTALK)

INGLIS:

I do, sir. As I transitioned from the active Air Force to the National Security Agency, I retained my affiliation with the reserve components and was pleased and proud to be able to serve in the Air National Guard for another 20 years.

ROGERS:

Great. Well, thank you for that service.

You mentioned in "queries of less than 300," what does -- what does that mean?

INGLIS:

In each of those cases, sir, there was a determination made an analyst at NSA that there was a reasonable, describable, articulable suspicion that an number of interest, a telephone number of interest, might be associated with a connected plot of a specific terrorist plot overseas, and therefore a desire to see whether that plot had a connection into the United States.

The process they go through then is as described, one where they make a -- a...

(CROSSTALK)

ROGERS:

Well, describe the inquiry -- it's not put -- you don't put in a name?

INGLIS:

We do not, sir.

ROGERS:

So you put in...

(CROSSTALK)

INGLIS:

The only thing we get from the providers are numbers. The only thing we could possibly then bounce against that data set are numbers, themselves.

ROGERS:

Right. So there are no names and no addresses affiliated with these phone numbers.

INGLIS:

No, there are not, sir.

ROGERS:

OK. Just phone numbers.

INGLIS:

That's right, sir.

ROGERS:

OK. Go ahead.

INGLIS:

So an analyst would then try to determine whether there was a describable, it must be written, documentation that would say that there is a suspicion that this is attributed to a foreign terrorist plot and there might be a U.S. nexus.

After having made that determination, they would make a further check to determine whether it is possible to discern that this might be associated with a U.S. person. The way you would infer that is you might look at the area code and say that area code could likely be in the United States. We all know that within this area, that if you see an area code that begins with 301, that would be Maryland. That would be your only insight into whether or not this might be attributable to a U.S. person.

If that were to be the case, then the case for a reasonable, articulable suspicious must get a further review to ensure that this is not a situation where somebody is merely expressing their First Amendment rights.

If that's all that was, if they were merely expressing their First Amendment rights, however objectionable any person might find that, that is not a basis to query the database.

If it gets through those checks, then at that point, it must be approved by one of those 20 plus two individuals -- 20 analysts, specially-trained analysts, or their two managers -- such that it might then be applied as a query against the data set. Again, the query itself would just be a number, and the query against the data set would then determine whether that number exists in the database. That's how that query is formed. And, again...

(CROSSTALK)

ROGERS:

So the response is not a name; it's an address. It's a phone number.

INGLIS:

It cannot be. If it were to be a name or if it were to be an address, there would be no possibility that the database would return any meaningful results, since none of that information is in the database.

ROGERS:

Just a phone number pops back up.

INGLIS:

Just a phone number. What comes back if you query the database are phone numbers that were in contact, if there are any, with that number. And, again, the other information in that database would indicate when that call occurred and what the duration of that call were -- were to be.

ROGERS:

Again, I just want to make very clear, there are no names and no addresses in that database.

INGLIS:

There are not, sir.

ROGERS:

OK. And why only less than 300 queries of phone numbers into that database?

INGLIS:

Sir, only less than 300 numbers were actually approved for query against that database. Those might have been applied multiple times, and therefore, there might be a number greater than that of actual queries against the database.

But the reason there are so few selectors approved is that the court has determined that there is a very narrow purpose for this -- this use. It can't be to prosecute a greater understanding of a simply domestic plot. It cannot be used to do anything other than terrorism. And so, therefore, there must be very well-defined describable written determinations that this is -- is a suspicion of a connection between a foreign plot and a domestic nexus. If it doesn't meet those standards...

(CROSSTALK)

ROGERS:

Are those queries reported to the court?

INGLIS:

Those queries are all reported to the Department of Justice, reviewed by the Department of Justice. The number of those queries are reported to the court. And any time that there is a dissemination associated with a U.S. person...

(CROSSTALK)

ROGERS:

Is there a court-approved process in order to make that query into that information of only phone numbers?

INGLIS:

Yes, sir. The court explicitly approves the process by which those determinations were made, and the Department of Justice provides a rich oversight auditing of that capability.

ROGERS:

Great. Thank you.

General Alexander, is the NSA on private company's servers as defined under these two programs?

ALEXANDER:

We are not.

ROGERS:

Is -- is the NSA have the ability to listen to Americans' phone calls or read their e-mails under these two programs?

ALEXANDER:

No, we do not have that authority.

ROGERS:

Does the technology exist at the NSA to flip a switch by some analyst to listen to Americans' phone

calls or read their e- mails?

ALEXANDER:

No.

ROGERS:

So the technology does not exist for any individual or group of individuals at the NSA to flip a switch to listen to Americans' phone calls or read their e-mails?

ALEXANDER:

That is correct.

ROGERS:

When -- Mr. Joyce, if you could help us understand that, if you get a piece of a number, there's been some public discussion that, gosh, there's just not a lot of value in what you might get from a program like this that has this many levels of oversight. Can you talk about how that might work into an investigation to help you prevent a terrorist attack in the United States?

JOYCE:

Investigating terrorism is not an exact science. It's like a mosaic. And we try to take these disparate pieces and bring them together to form a picture. There are many different pieces of intelligence. We have assets. We have physical surveillance. We have electronic surveillance through a legal process; phone records through additional legal process; financial records.

Also, these programs that we're talking about here today, they're all valuable pieces to bring that mosaic together and figure out how these individuals are plotting to attack the United States here or whether it's U.S. interests overseas.

So, every dot, as General Alexander mentioned, we hear the cliche frequently after 9/11 about connecting the dots. I can tell you as a team, and with the committee and with the American public, we come together to put all those dots together to form that picture to allow us to disrupt these activities.

ROGERS:

Thank you.

Given the large number of questions by members, I'm going to move along.

Mr. Ruppersberger, for a brief...

RUPPERSBERGER:

Firstly, I want to thank all the witnesses for your presentation, especially Mr. Cole -- a very good presentation. I think you explained the law in a very succinct way.

You know, it's unfortunate sometimes when we have incidents like this that a lot of negative or false information gets out. I think, though, that those of us who work in this field, in the intelligence field every day, know what the facts are and we're trying to now present those facts through this panel. That's important.

But I would say that I weren't in this field and if I were to listen to the media accounts of what occurred

in the beginning, I would be concerned, too. So, this is very important that we get the message out to the American public that what we do is legal and we're doing it to protect our national security from attacks from terrorists.

Now, there are -- one area that, Mr. Litt, you -- you addressed this -- but I think it's important to just reemphasize the FISA court. You know, again, it's unfortunate, when people disagree with you, they attack you. They say things that aren't true. We know that these are federal judges in the FISA court. They have integrity, and that they will not approve anything that they feel is wrong. We have 90-day periods where the court looks at this issue.

I want to ask you, though, General Alexander, do you feel in any way that the FISA court is a rubber-stamp based on the process? Our forefathers created a great system of government, and that's checks and balances. And that's what we are. That's what we do in this country to follow our Constitution. It's unfortunate that these federal judges are being attacked.

ALEXANDER:

I do not. I believe, as you have stated, the federal judges on that court are superb. Our nation would be proud of what they do and the way they go back and forth to make sure we do this exactly right.

And every time we make a mistake, how they work with us to make sure it is done correctly to protect our civil liberties and privacy and go through the court process. They have been extremely professional. There is, from my perspective, no rubber-stamp.

It's kind of interesting. It's like saying you just ran a 26- mile marathon; somebody said, "Well, that was just a jog." Every time we work with the court, the details and the specifics of that that go from us up through the FBI, through the Department of Justice and through the court on each one of those orders that we go to the court. There is tremendous oversight, compliance and work. And I think the court has done a superb job.

More importantly, if I could, what we worked hard to do is to bring all of these -- all these under court supervision for just this reason. I mean, we've done the right thing, I think, for our country here.

Thank you.

RUPPERSBERGER:

Thank you for that answer.

The second area I want to get into, General Alexander, the public are saying, "Well, how did this happen?" We have -- we have rules. We have regulations. We have individuals that work in intelligence go through being -- persistently being classified. And yet here we have a technical person who had lost some jobs; had a background that wouldn't always would be considered the best.

We have to learn from mistakes how they've occurred. What system are you or the director of national intelligence of the administration putting into effect now to make sure what happened in this situation, that if another person were to -- to turn against his or her country, that we would have an alarm system that would not put us in this position right now?

ALEXANDER:

So, this is a very difficult question, especially when that person is a system administrator and they get

great access...

RUPPERSBERGER:

Why don't you say what a system administrator is?

ALEXANDER:

Well, a system administrator is one that actually helps operate, run, set the conditions, the auditing and stuff on a system or a portion of the network. When one of those persons misuses their authorities, this is a huge problem.

So working with the director of national intelligence, what we are doing is working to come up with a two-person rule and oversight for those, and ensure that we have a way of blocking people from taking information out of our system. This is work in progress. We're working with the FBI on the investigation. We don't have all the facts yet. We've got to get those. And as we're getting those facts, we are working through our system. Director Clapper has asked us to do that and providing that feedback back to the rest of the community.

RUPPERSBERGER:

OK. Thank you.

I yield back.

ROGERS:

(OFF-MIKE)

THORNBERRY:

Thank you, Mr. Chairman.

And thank you all for being here, and for making some additional information available to the public. I know it's frustrating for you, as it is for us, to have these targeted narrow leaks and not be able to talk about the bigger picture.

General Alexander, you mentioned that you're going to send us tomorrow 50 cases that have been stopped because of these programs, basically. Four have been made public to this point. And I think there are two new ones that you are talking about today. But I would invite you to explain to us both of those two new cases -- Mowlin (ph) and the Operation WiFi case. And one of them starts with a 215; one of them starts with a 702.

And so I think it's important for you to provide the information about how these programs stopped those terrorist attacks.

ALEXANDER:

OK. I'm going to defer this, because the actual guys who actually do all the work and (inaudible) is the FBI, and get it exactly right. I'm going to have Sean do that. Go ahead, Sean.

JOYCE:

So, Congressman, as I mentioned previously, NSA on the Op WiFi, which is Khalid Ouazzani out of Kansas City. That was the example that I referred to earlier. NSA, utilizing 702 authority, identified an extremist located in Yemen. This extremist located in Yemen was talking with an individual located

inside the United States in Kansas City, Missouri. That individual was identified as Khalid Ouazzani.

The FBI immediately served legal process to fully identify Ouazzani. We went up on electronic surveillance and identified his co-conspirators. And this was the plot that was in the very initial stages of plotting to bomb the New York Stock Exchange. We were able to disrupt the plot. We were able to lure some individuals to the United States. And we were able to effect their arrest. And they were convicted for this terrorist activity.

THORNBERRY:

OK. Just so I -- on that plot, it was under the 702, which is targeted against foreigners, that some communication from this person in Yemen back to the United States was picked up. And then they turned it over to you at the FBI to serve legal process on this person in the United States.

JOYCE:

That is absolutely correct. And if you recall, under 702, it has to be a non-U.S. person outside the United States, and then also one of the criteria is linked to terrorism.

THORNBERRY:

OK. Would you say that this -- their intention to blow up the New York Stock Exchange was a serious plot? Or is this something that they kind of dreamed about, you know, talking among their buddies?

JOYCE:

I think the jury considered it serious, since they were all convicted.

THORNBERRY:

OK. And -- and what about the other plot? October, 2007, that started I think with a 215?

JOYCE:

I refer to that plot. It was an investigation after 9/11 that the FBI conducted. We conducted that investigation and did not find any connection to terrorist activity. Several years later, under the 215 business record provision, the NSA provided us a telephone number only, in San Diego, that had indirect contact with an extremist outside the United States.

We served legal process to identify who was the subscriber to this telephone number. We identified that individual. We were able to, under further investigation and electronic surveillance that we applied specifically for this U.S. person with the FISA court, we were able to identify co-conspirators and we were able to disrupt this terrorist activity.

THORNBERRY:

I'm sorry. Repeat for me again what they were plotting to do.

JOYCE:

He as actually -- he was providing financial support to an overseas terrorist group that was a designated terrorist group by the United States.

THORNBERRY:

But there was some connection to suicide bombings that they were talking about, correct?

JOYCE:

Not in the example that I'm citing right here.

THORNBERRY:

Oh, I'm sorry, the group in Somalia to which he was financing, that's what they -- that's what they do do in Somalia, correct?

JOYCE:

That is correct, and as you know, as part of our classified hearings regarding the American presence in -- in that area of the world.

THORNBERRY:

OK. OK, thank you.

Chairman (OFF-MIKE)

ALEXANDER:

If I could, Congressman, just -- just hit a couple key points. It's over 50 cases. And the reason I'm not giving a specific number is we want the rest of the community to actually beef those up and make sure that (inaudible) we have there is exactly right. I'd give you the number 50X. But if somebody says, "Well, not this one." Actually, what we're finding out is there are more. They said, "You missed these three or four." So those are being added to the packet.

On the top of that packet we'll have a summary of all of these, the listing of those. I believe those numbers are things that we can make public, that you can use, that we can use. And we'll try to give you the numbers that apply to Europe, as well, as well as those that had a nexus in the United States.

The issue on terms of releasing more on the specific overseas cases is (inaudible) our -- it's our concern that in some of those -- now, going into further details of exactly what we did and how we did it may prevent us from disrupting a future plot.

So that's something that work in progress. Our intent is to get that to the committee tomorrow for both -- both Intel Committees for the Senate and House.

THORNBERRY:

Great. Thank you.

ROGERS:

Mr. Thompson?

THOMPSON:

Thank you, Mr. Chairman.

Thank you all very much for being here and for your testimony and for your service to our country.

Mr. Litt, before going to a hearing, does or has the FISA court ever rejected a case that's been brought before it?

LITT:

I believe the answer to that is yes, but I would defer that to the deputy attorney general.

COLE:

It has happened. It's not often, but it does happen.

THOMPSON:

Thank you.

Mr. Cole, what kinds of records comprise the data collected under the business records provision?

COLE:

There's a couple of different kinds. The shorthand -- and it's required under the statute -- is the kinds of records you could get with a grand jury subpoena. These are business records that already exist. It could be a contract. It could be something like that.

In this instance that we're talking about for this program, these are telephone records. And it's just like your telephone bill. It'll show a number called, the date the number was called, how long the call occurred; a number that called back to you. That's all it is, not even identifying who the people are that's involved.

THOMPSON:

Have you previously collected anything else under that authority?

COLE:

Under the 215 authority?

THOMPSON:

Correct.

COLE:

I'm not sure beyond the 215 and the 702 that -- answering about what we have and haven't collected has been declassified to be talked about.

THOMPSON:

OK.

It was said that there's been cases where there was data inadvertently or mistakenly collected and then subsequently destroyed. Is that...

COLE:

That's correct.

THOMPSON:

And -- and there actually has been data that has been inadvertently collected and it was destroyed, nothing else was done with it?

COLE:

That's correct. The -- this is a very strict process that we go through in that regard. You can get a wrong digit on a phone number and you collect the wrong number, something like that. And when that's

discovered, that's taken care of in that way.

THOMPSON:

And who does the checking? Who -- who determines if something has been inadvertently collected and then decides that it's -- needs to be destroyed?

COLE:

Well, I'll -- I'll refer over to NSA in the first instance, because they do a very robust and vigorous check internally themselves. But then as an after-the-fact, the Department of Justice and ODNI and the inspector general for NSA also do audits and make sure that we understand all the uses. And if there's any compliance problems that they're identified, that they're given to the court, they're given to the Congress, and they're fixed.

THOMPSON:

I -- I don't think I need anything more than -- than that.

General Alexander, can you tell us what Snowden meant during this chat thing that he did when he said that NSA provides Congress with, and I quote, "a special immunity to its surveillance"?

ALEXANDER:

I have no idea.

THOMPSON:

Anybody else?

ALEXANDER:

I'm not sure I understand the context of the special immunity.

THOMPSON:

I -- I don't either. That's why...

(CROSSTALK)

ALEXANDER:

We treat you with special respect.

(LAUGHTER)

THOMPSON:

He said with a "special immunity to its surveillance."

ALEXANDER:

I -- I have no idea. I think it may be in terms of disseminating any information, let's say, not in this program but in any program that we have, if we have to disseminate U.S. persons data or a threat to a U.S. member of Congress, we're not allowed to say the name unless it's valuable to one of the investigations or (inaudible).

So we can't just put out names and stuff in our things (ph). So part of the minimization procedures protects the who.

Did you want to add to that?

INGLIS (?):

No, I would simply have said that your status as U.S. persons gives you a special status, as we've described throughout this hearing.

THOMPSON:

If you -- if that does surface and you do figure that out you'll get that information to us?

Also the president kind of suggested, I guess, in his television interview the other night that the New York subway bomber could not have been or would not have been caught without PRISM. Is that true?

JOYCE:

Yes, that is accurate. Without the 702 tool we would not have identified Najibullah Zazi.

THOMPSON:

Thank you. I have no further question.

I yield back the balance of my time.

ROGERS:

Mr. Miller?

MILLER:

Thank you, Mr. Chairman.

General Alexander, which agency actually presents the package to the FISA court for them to make their decision?

ALEXANDER:

Well, it's actually -- business records, FISA, it's the FBI (inaudible).

Go ahead.

JOYCE:

The FBI is part of the process. It then goes over to the Department of Justice. And they are the ones -- if the DAG wants to comment on that.

COLE:

The formal aspect of the statute allows the director of the FBI to make an application to the court. The Justice Department handles that process. We make the -- put all the paperwork together. And it must be signed off on before it goes to the court by either the attorney general, myself, or if we have a confirmed assistant attorney general in charge of the National Security Division, that person is authorized. But it has to be one of the three of us to sign it before it goes.

MILLER:

The court is a single judge?

COLE:

The judges sit kind of in -- in rotation in the court presiding over it. These are all Article 3 judges. They have lifetime appointments. They have their districts that they deal with, and they are selected by the chief justice to sit on the FISA court for a period of time. And so they will rotate through and be the duty judges that are required for this.

MILLER:

I guess the crux of my question is, would there be a way that if you did not get the answer that you wanted from a certain judge could you go to another FISA court judge and ask for another opinion?

COLE:

I -- I think that would be very, very difficult to do, because the staff at the FISA court does a great deal of the prep work and they're gonna recognize when they've thrown something back that if you're coming back and you haven't made any changes to correct the deficiencies that caused them to throw it back, my guess is they'll throw it back again.

MILLER:

And I think one of the things that a lot of people don't understand -- and it was alluded to by Mr. Litt; and I think, Mr. Cole, you have also discussed it -- and that's the read-ahead document that the court gets, the opportunity. A lot of focus has been made on the fact that as my colleague, Mr. Thompson said, court's a rubberstamp. But they do have an opportunity to review the documents prior to rendering a decision.

COLE:

They do. And it's by no means as a rubber stamp. They push back a lot. And when they see something -- these are very thick applications that have a lot in them. And when they see anything that raises an issue, they will push back and say, "We need more information about this area. We need more information about that legal issue. We need more information about your facts in certain areas.'

This is by no means a rubberstamp. There is an enormous amount of work. And they make sure -- they're the ones to make sure that the privacy and the civil liberty interests of United States' citizens are honored. They're that bulwark in this process. So they -- they have to be satisfied.

MILLER:

There's been some discussion this morning on the inadvertent violation of a court order where data has been collected and then destroyed. But has there ever been any disciplinary action taken on somebody who inadvertently violated an order?

COLE:

Not that I'm aware of. And I think one of the statistics that Mr. Inglis had included in his comment was that in the history of this, there has never been found an intentional violation of any of the provisions of the court order, or any of the collection in that regard. So the -- the nature of the kinds of anomalies that existed were technical errors, were typographical errors, things of that nature as opposed to anything that was remotely intentional. So there would be in those instances, no reason for discipline. There may be reason to make sure our systems are fixed so that a technical violation, or technical error doesn't exist again because we've identified it. But nothing intentional.

LITT:

Can I just add one thing to that point? An important part of the oversight process that the Department of Justice, and the ODNI engage in is when compliance problems are identified, and the vast majority of them are self-identified by NSA, but when a compliance issue is identified, we go and look at it and say, OK are there changes that need to be made in the system so that this kind of mistake doesn't happen again? It's a constantly improving process to prevent problems from occurring.

MILLER:

Thank you. I yield back.

ROGERS:

Ms. Schakowsky?

SCHAKOWSKY:

Thank you Mr. Chairman. General Alexander, do you feel that this open hearing today jeopardizes in any way our national security?

ALEXANDER:

I don't think the sharing itself jeopardizes it. I think the damage was done in the release of the information already. I think today what we have the opportunity is (sic) so where it makes sense, provide additional information on the oversight, the compliance and some of the -- the statistics, without jeopardizing it. So to answer your question, no. We're being very careful to do that, and I appreciate what the committee has done on that.

SCHAKOWSKY:

How many people were in the same position as Snowden was, as a systems manager to have access to this information that could be damaging if released?

ALEXANDER:

Well, there are system administrators throughout NSA and in our -- all our complexes around the world. And there is on the order of a thousand system administrators, people who actually run the networks that have, in certain sections, that -- that level of authority and ability to interface with...

SCHAKOWSKY:

How many of those are outside contractors, rather than...

ALEXANDER:

The majority are contractors. As you may know, as you may recall, about 12-13 years ago as we tried to downsize our government work force, we pushed more of our information technology workforce or system administrators to the contract arena. That's consistent across the intelligence community.

SCHAKOWSKY:

I would -- I would argue that this conversation that we're having now could have -- could have happened unlike what you said Mr. Litt. And perhaps we disagree also, General Alexander, that the erosion of trust, the misconceptions and the misunderstandings that resulted and why would assume that when there's 1,000 -- are there any more than 1,000 by the way?

ALEXANDER:

Well, we're actually counting all of those positions. I'll get you an accurate number.

SCHAKOWSKY:

That -- that some of this information would not have become public. And that the effort that has to convince the American public of the necessity of this program, I think would suggest that we would have been better off at having a discussion of vigorous oversight, the legal framework, et cetera up front, and how this could prevent perhaps another 9/11, and in fact, 50 or so, attacks. Let me ask you this, Mr. Cole, you know you -- you were talking about transparency, and you were saying that -- essentially that while the Verizon phone records order looked bad on its face, that there are other FISA court orders that talk in more depth about the legal rationale, about -- about what we're -- what we're doing.

So, will you release those court opinions with the necessary redactions, of course? And if not, why?

COLE:

Well, I'm going to refer that over to Mr. Litt because the classifying authority on that would be DNI.

LITT:

As you may know, we have been working for some time on trying to declassify opinions of the FISA court. It's been a very difficult task, because like most legal opinions, you have facts intermingled with legal discussion. And the facts frequently involve classified information, sensitive sources and methods. And what we've been discovering is that when you remove all of the information that needs to be classified, you're left with something that looks like Swiss cheese, and is not really very comprehensible. Having said that, I think as -- as General Alexander said, there's information out in the public domain now. There's -- the director of national intelligence declassified certain information about these programs last week.

And as a result of that, we are going back, taking another look at these opinions to see whether, in light of that declassification, there's now -- we can make a more comprehensible release of the opinion. So the answer to that is, we are looking at that and -- and frankly we would like to release it to the public domain, as much of this as we can, without compromising national security.

SCHAKOWSKY:

I think -- General Alexander, so what other types of -- of records are collected under this Section 215? Can -- can you talk about that at all?

ALEXANDER:

Yeah, for NSA the only -- the only records that are collected under business records 215 is this telephony data. That's all.

SCHAKOWSKY:

And is there authorization to collect more?

ALEXANDER:

Under 215 for us? No, this is the only -- that we do. Now it gets into other authorities, but it's not ours. And I don't now if the -- I'll pass that to the attorney general because you're asking me now outside of

NSA.

COLE:

215 is generally -- is a general provision that allows the acquisition of business records if its relevant to a national security investigation. So that showing has to be made to the court to allow that subpoena to issue that there is a relevance, and a connection. And that can be any -- any number of different kinds of records that a business might maintain; customer records, purchase orders, things of that nature. Somebody buys materials that they could buy an explosive out of, you could go to a company that sells those and get records of the purchase. Things of that nature.

SCHAKOWSKY:

What about e-mails?

COLE:

E-mails would not be covered by business records in that regard. You would have to -- under the Electronic Communications Privacy Act, you get specific court authorization for e-mails, that's stored content. If you're going to be looking at them in real time while they're going, you're going to have a separate FISA court order that would allow you to do that. It wouldn't be covered by the business records.

SCHAKOWSKY:

Thank you Mr. Chairman.

ALEXANDER:

Could I just make sure -- one clear part on the system administrator versus -- so what you get access to is helping to run the network, and the web servers that are on that network that are publicly available. To get to any data, like the business records 215 data that we're talking about, that's in an exceptionally controlled area. You would have to have specific certificates to get into that. I am not aware that he had -- he, Snowden, had any access to that. And on the reasonable articulable suspicion numbers and on what we're seeing there, I don't know of any inaccurate RAS numbers that have occurred since 2009.

There are rigorous controls that we have from a technical perspective that once the numbers can -- is considered RAS-approved, that you put that number in. You can't make a mistake because the system helps correct that now. So that -- that is a technical control that we have put in there.

SCHAKOWSKY:

Thank you. I yield back.

CONAWAY:

Well, thank you gentlemen. General Alexander thank you for your long service. Mr. Cole and Mr. Inglis went through -- through a very extensive array of the oversight and internal controls that are associated with -- with what's going on. In a business environment, Sarbanes-Oxley requires that companies go through their entire system to make sure that, not only do the details trees work, but that the forest works as well. Is there any one at -- in the vast array of what you guys are doing that steps back and says, all right, we're -- the goal is to protect privacy and our civil liberties and we're doing the very best we can.

Is there a -- an internal control audit, so to speak that looks at the entire system that says, we've got the waterfront covered? And we're doing what we need to do?

COLE:

I'll start. I mean there are these periodic reviews that I've described that audit everything that is done under both of these programs by both NSA and the Department of Justice, and the Office of the Director of National Intelligence, and we report to the court, and we report to Congress. So all of that is done looking at the whole program at the same time.

CONAWAY:

I guess I -- Mr. Cole I'm looking at the -- the program of that. I understand that those pieces work really well, and that that's their design to -- to go at it and create the -- that kind of audit process. But is there an overall look at -- at everything that is done to say, we've got it all covered? Or -- and if we don't, and there are suggestions that we need to improve it, where do those suggestions get vetted? And have we had suggestions for improvement that we said, no, we don't need to do that?

LITT:

Mr. Conaway if I might speak on that, there are at least two levels at which that takes place.

One is by statute within the Office of the Director of National Intelligence, there is -- there is a civil liberties protection officer -- his name is Alex Joel, who's an incredibly capable person whose job it is to take exactly that kind of look at our programs and make suggestions for the protection of civil liberties.

Outside of -- of the intelligence community, there...

(CROSSTALK)

CONAWAY:

And that person would have the requisite clearances to know all the details?

(CROSSTALK)

LITT:

Absolutely. He is -- he is, in fact, part of this audit process as well, his office is.

The second thing is that -- is that outside of the intelligence community, the president's Civil Liberties Oversight Board, which has -- has five confirmed members is also charged with evaluating the impact of our counterterrorism programs on privacy and civil liberties.

They also have full clearances. They have the ability to get full visibility into this program. In fact, they have recently been briefed on these programs, and I know they are, in fact, looking at them to make exactly that kind of assessment.

(CROSSTALK)

CONAWAY:

And who -- who do they report to? Is that report public?

LITT:

It's the president's board. I suspect that to the extent they're making a classified report, it would not be

public. To the extent that they can make an unclassified report, it's up to them whether or not it becomes public.

CONAWAY:

Several of you mentioned the term "minimization" and then also five-year destruction, rolling five-year window on the -- on the business record issues. You've used the word "purge," "get rid of," "destroy."

In an electronic setting, can you help us understand exactly what that means? I understand when I shred a piece of paper into the thousand-and-one pieces, that's one thing. But given the number of times you back up data and all the other, can a citizen feel like that once the minimization worked, that this electronically, we have in fact deleted all these things that are -- that we're supposed to delete?

INGLIS:

So I'll start at that. Yes, sir, I believe that we can. We have a fairly comprehensive system at NSA that whenever we collect anything, whether it's under this authority or some other, we actually bind to that communication where we got it, how we got it, what authority we got it under so that we know precisely whether we can retain it for some fixed period of time.

And if it simply ages off, as in the case of the B.R. FISA data we talked about, at the expiration of those five years, it is automatically taken out of the system. Literally just deleted from the system.

CONAWAY:

OK. And it's mechanically overwritten and all of the back-up copies of that are done away with, and...

INGLIS:

Yes, sir.

CONAWAY:

OK.

INGLIS:

It's -- it gets fairly complicated very quickly, but we have what are called source systems of record within our architecture, and those are the places that we say if it -- if the data element has the right to exist, it's attributable to one of those. And if it doesn't have the right to exist, you can't find it in there.

And we have very specific lists of information that determine what the provenance of data is, how long that data can be retained. We have on the other side of the coin purge lists that if we were authorized -- if we were required to purge something, that item would show up explicitly on that list. And we regularly run that against our data sets to make sure that we've checked and double-checked that those things that should be purged have been purged.

CONAWAY:

All right.

One quick one: Any indication that the -- the FISA court has a problem with resources necessary to run its oversight piece?

INGLIS:

Not that I'm aware of right now. But, obviously, the courts are suffering under sequestration, like

everybody else. So I don't know what's gonna hit them as we go forward.

CONAWAY:

Thank you, sir,

I yield back.

ROGERS:

Mr. Conaway.

Mr. Langevin?

LANGEVIN:

Thank you, Mr. Chairman.

And gentlemen, I want to thank you all for your testimony here today and for your service to our -- our country.

I'm -- as members of the committee, I have been briefed on the program, and -- and I know the excess of due diligence you've gone through to make sure that this is done right.

So I think it's important that this discussion is being had this morning. And hopefully it's gonna give greater confidence to the American people that all the agencies involved have dotted their i's and crossed their t's.

I especially think it's helpful that we have the discussion about the FISA court today and -- and how detailed the -- the requests have to be before they get approval and it's made clear that these are not just one-page documents that are presented to a FISA judge and then it's rubber stamped.

It actually goes through excessive due diligence, and -- and before it even gets to the point where the judge sees it. And, obviously, if the -- if all the criteria have been met, then it gets -- it gets approved, and if it's -- if the criteria have not been met, it's gonna be rejected.

So, I won't belabor that point, excepting that's been had -- been a very fruitful discussion.

But can you talk further about the -- again the role of the I.G. and go into that -- that -- that process a little more so that the -- the amount of review the I.G. does, once a query has been made in terms of the range of queries that have been made, I think that's -- would be important to clarify.

INGLIS:

I would just start with that, and then defer to the ODNI and the attorney general -- deputy attorney general for some followup.

And so, at NSA, any analyst that wants to form a query, regardless of whether it's this -- this authority or any other, essentially has a two-person control rule. They would determine whether this query should be applied, and there's someone who provides oversight on that.

We've already learned that under the metadata records that are captured by the B.R. FISA program, that there's a very special court- defined process by which that's done.

Those are all subject to the I.G., the inspector general's review on a periodic basis, such that we can look at the procedures as defined, the procedures as executed, reconcile the two and ensure that

internal to NSA, that that's done exactly right. There are periodic reports that the I.G. has to produce on these various programs, and they are faithfully reported.

But I think the real checks and balances within the executive branch happen between NSA and the Department of Justice, the Office of the Director of National Intelligence. And because NSA also has a foot within the Department of Defense, the Department of Defense enters into that as well. They have intelligence oversight mechanisms.

And between those four components, there is rich and rigorous oversight which varies in terms of the things that they look for, based upon the authorities. B.R. FISA is a particularly rigorous authority. But they all have checks and balances to transcend just NSA.

LANGEVIN:

OK.

COLE (?):

And, Congressman, if I -- if I could add to that, and I refer you to a recent review by the DOJ inspector general on the 702 program that was highly complimentary of all the checks and balances that were in place.

LANGEVIN:

Thank you.

So let me turn my attention now to -- I know these programs primarily target non-U.S. persons, but can you -- and this is probably a question for you, Mr. Joyce, just to clarify, you've said that if a U.S. person or a -- the overseas or the United States or a non-U.S. person living in the United States, that if they're -- we become aware that they may be involved in terrorist activity that they are served -- processed.

Can you go into that level of detail of what then happens and how the courts are involved with -- if we become aware that a U.S. person is involved?

JOYCE:

So -- so I think either -- maybe I misspoke or -- or you misspoke. We -- we -- we are not looking at all at U.S. persons. The 702 is anyone outside the United States. And even if a U.S. person is outside of the United States, it does not include it in the 702 coverage.

OK, so it's a non-U.S. person outside the United States, and it has to have -- there's three different criteria it goes through. One of those links is terrorism. So that is where specifically only certain individuals are targeted. Those ones, one of the criteria, linked to terrorism.

On numerous occasions, as I've outlined in some of the examples, those individuals outside the United States were discovered communicating with someone inside the United States.

We then -- that is, being tipped from the NSA. We then go through the legal process here, the FBI does, regarding that U.S. person. So we go and we have to serve what's called a national security letter to identify the subscriber. It's much like a subpoena.

Following that, if we want to pursue electronic surveillance, we have to make a specific application

regarding that person with the FISA court here.

LANGEVIN:

That's what I was looking for. So thank you very much.

I yield back.

(OFF-MIKE)

ALEXANDER:

Sir, if I could, just to follow on and -- and to clarify, 'cause as we're going through this, I want to make sure that everything we say is exactly right -- from from my perspective. And so, as Sean said, NSA may not target the phone calls or e-mails of any U.S. person anywhere in the world without individualized court orders.

LANGEVIN (?):

OK. Thank you.

ROGERS:

That's an important point we can't make enough.

Mr. Lobiondo?

LOBIONDO:

Thank you. Thank you, Mr. Chairman.

General Alexander and team, thank you for helping -- helping us understand in so many closed sessions and hopefully helping the nation understand what we're doing, why we're doing it, and how we're doing it.

I want to focus a little bit more on 702, if we could.

And, General Alexander, could you -- could you explain what happens if a target of surveillance is communicating with a U.S. person in the United States?

ALEXANDER:

So, under 702, I think the best case is some that Sean Joyce made. If we see, if we're tracking a known terrorist in another country, say Pakistan, Yemen or someplace, and we see them communicating with someone in the United States, and it has a terrorism nexus, focused on doing something in the United States, we tip that to the FBI.

So our job is to identify, see the nexus of it. It could be in another country as well. So sometimes, we'd see somebody in that -- one of those countries planning something in Europe or elsewhere. We would then share that through intelligence meetings to those countries.

But when it comes into the United States, our job ends. We're the outside and we provide that to the inside FBI to take it from there. So they, then, take it and say, "Does this make sense?" They'll go up, as Sean explained, look at the process for getting additional information to see if this is a lead worth following.

LOBIONDO:

And what does the government have to do if it wants to target a U.S. person under FISA when they're located abroad -- when they're not here? What -- what would be the process for the government?

COLE:

That would be the -- a full package going to the FISA court, identifying that person; identifying the probable cause to believe that that person is involved in either terrorism or foreign intelligence activities; and indicating that we have then the request to the court to allow us to intercept their communications because we've made the showing that they're involved in terrorist or foreign intelligence activities.

So we'd have to make a formal application targeting that person specifically, whether they're inside or outside of the United States.

LOBIONDO:

And what if you...

(CROSSTALK)

INGLIS:

And, sir, if I might. And again, that could not be done under 702. There's a separate section of the Foreign Intelligence Surveillance Act that would allow that, but it would not be doable under 702.

LOBIONDO:

And -- and what if you want to monitor someone's communication in the United States?

COLE:

Same thing. Again, a different provision of FISA, but we would have to show that that person is in fact with probable cause involved in foreign terrorist activities or foreign intelligence activities on behalf of a terrorist organization or a foreign power. We'd have to lay out to the court all of those facts to get the court's permission to then target that person.

LOBIONDO:

So, I just want to reemphasize that. You -- you have to specifically go to the FISA court and make your case as to why this information is necessary to be accessed.

COLE:

That's correct.

LOBIONDO:

And without that, you have no authority and cannot do it and do not do it.

COLE:

That's correct.

LOBIONDO:

OK. Thank you.

I yield back, Mr. Chairman.

ROGERS:

Great. Thank you very much.

Mr. Schiff?

SCHIFF:

Thank you, Mr. Chairman.

And thank you, gentlemen, for your work.

On the business records program, the general FISA court order allows you to get the metadata from the communications providers. Then when there are reasonable and articulable facts, you can go and see if one of the numbers has a match in the metadata.

On those 300 or so occasions when you do that, does that require separate court approval? Or does the general FISA court order allow you, when your analysts have the reasonable, articulable facts, to make that query? In other words, every time you make the query, does that have to be approved by the court?

COLE:

We do not have to get separate court approval for each query. The court sets out the standard that must be met in order to make the query, in its order. And that's in the primary order. And then that's what we audit in a very robust way in any number of different facets through both executive branch and then give it to the court, and give it to the Congress.

So we're given that 90-day period with these parameters and restrictions to access it. We don't go back to the court each time.

SCHIFF:

And does the court scrutinize after you present back to the court, "these are the occasions where we found reasonable articulable facts," do they scrutinize your basis for conducting those queries?

COLE:

Yes, they do.

SCHIFF:

General Alexander, I wanted to ask you. I raised this in closed session, but I'd like to raise it publicly as well. What are the prospects for changing the program such that rather than the government acquiring the vast amounts of metadata, the telecommunications retain the metadata, and then only on those 300 or so occasions where it needs to be queried, you're querying the telecommunications providers for whether they have those business records related to a reasonable articulable suspicion of foreign terrorist connection?

ALEXANDER:

I think jointly the FBI and NSA are looking at the architectural framework of how we actually do this program and what are the advantages and disadvantages of doing each one. Each case, as you know from our discussions, if you leave it at the service providers, you have a separate set of issues in terms of how you actually get the information, then how you have to go back and get that information, and how you follow it on and the legal authority for them to compel them to keep these records for a certain

period of time.

So what we're doing is we're going to look at that and come back to the director of national intelligence, the administration and then to you all, and give you recommendations on that for both the House and the Senate. I do think that that's something that we've agreed to look at and that we'll do. It's just going to take some time. We want to do it right.

And I think, just to set expectations, the -- the concern is speed in crisis. How do we do this? And so that's what we need to bring back to you, and then I think have this discussion here and let people know where we are on it.

Anything that you wanted to add?

SCHIFF:

I would -- I would strongly encourage us to vigorously investigate that potential restructuring. Even though there may be attendant inefficiencies with it, I think that the American people may be much more comfortable with the telecommunications companies retaining those business records, that metadata, than the government acquiring it, even though the government doesn't query it except on very rare occasions.

ALEXANDER:

So it may be something like that that we'd bring back and look at. So we are going to look at that. And we have already committed to doing that and we will do that, and go through all the details of that.

SCHIFF:

Mr. Litt, I wanted to ask you about the FISA court opinions. This week, I'm going to be introducing the House companion to the bipartisan Merkley bill that would require disclosure of certain FISA court opinions, again, in a form that doesn't impair our national security.

I recognize the difficulty that you described earlier in making sure those opinions are generated in a way that doesn't compromise the programs. You mentioned that you're doing a review, and I know one's been going on for sometime. In light of how much of the programs have now been declassified, how soon do you think you can get back to us about whether you're going to be able to declassify some of those FISA court opinions?

LITT:

I'm hesitant to answer any question that begins "how soon," partly because there are a lot of agencies with equities in this, partly because there's a lot else going on in this area. My time has not been quite as free-up to address this topic as I would have liked over the last week-and-a-half.

I can tell you that -- that I've asked my staff to work with the other agencies involved and try to press this along as quickly as possible. We're trying to identify those opinions where we think there's the greatest public interest in having them declassified, and start with those. And we'd like to push the process through as quickly as possible at this point.

SCHIFF:

And I would just encourage in the last second that beyond the two programs at issue here, to the degree you can declassify other FISA court opinions, I think it's in the public interest.

LITT:

Yes, I think that's part of what we're doing.

SCHIFF:

Thank you, Mr. Chairman.

COLE:

Congressman Schiff, I just wanted to correct a little bit one of the things I said. The FISC does not review each and every reasonable, articulable suspicion determination. What does happen is they are given reports every 30 days in the aggregate. And if there are any compliance issues, if we found that it wasn't applied properly, that's reported separately to the court.

ROGERS:

Do you have a followup?

SCHIFF:

Thank you, Mr. Chairman. I just want to make sure I understood what you just said. A prior court approval is not necessary for a specific query. But when you report back to the court about how the order has been implemented, you do set out those cases where you found reasonable articulable facts and made a query. Do you set out those with specificity or do you just say "on 15 occasions, we made a query"?

COLE:

It's more the latter -- the aggregate number where we've made a query. And if there's any problems that have been discovered, then we with specificity report to the court those problems.

SCHIFF:

It may be worth considering providing the basis of the reasonable and articulable facts and having the court review that as a -- as a further check and balance. I'd just make that suggestion.

ROGERS:

Mr. Cole, my understanding, though, is that every access is already preapproved; that the way you get into the system is court- approved. Is that correct?

COLE:

That's correct.

The court sets out the standards which have to be applied to allow us to make the query in the first place. Then the application -- the implementation of that standard is reviewed by NSA internally at several levels before the actual implementation is done. It's reviewed by the Department of Justice. It's reviewed by the Office of the Director of National Intelligence. It's reviewed by the inspector general for the National Security Agency. So there's numerous levels of review of the application of this. And if there are any problems with those reviews, those are then reported to the court.

ROGERS:

And -- and just to be clear, so if they don't follow the court-approved process, that would be a

variation, that would have to be reported to the court?

COLE:

That's correct.

ROGERS:

OK. But you are meeting the court-approved process with every query?

COLE:

That's correct.

INGLIS:

And sir, if I might add to that that every one of those query is audited, those are all reviewed by the Department of Justice. Those are the reviews that we spoked about -- spoke about at 30 and 90 days. And there's a very specific focus on those that we believe are attributable to U.S. persons despite the fact that in (inaudible) FISA we don't know the identities of those persons. And so the court gets all of those reports.

SCHIFF:

Thank you, Mr. Chairman.

I -- I just point out, all those internal checks are valuable, but they're still internal checks. And it may be worthwhile having the court, if not prospectively at least after the fact review those determinations.

Thank you, Mr. Chairman.

NUNES:

Thank you, Mr. Chairman.

Mr. Cole, really what's happened here is that the totality of many problems within the executive branch has now tarnished the fine folks at the NSA and the CIA. And I just made a short list here, but, you know, right after Benghazi there was -- there's lies after Benghazi, four dead Americans. Fast and Furious, the Congress still is missing documents. We have dead Americans and dead Mexican citizens. You at least tapped into or got phone records from AP reporters, Fox News reporters, including from the House Gallery right here within this building.

Last week, as you know, A.G. Holder has been -- is being accused by the Judiciary Committee of possibly lying to the committee.

And then to top it all off, you have, you know, an IRS official who with other officials ran like a covert media operation on a Friday to help, you know, try to release documents to think that this would just go away about the release of personal data from U.S. citizens from the IRS.

So now -- you know, I understand when my constituents ask me, "Well, if the IRS is leaking personal data" -- General Alexander, this question's for you -- "how do I know for sure that the NSA and the -- and (inaudible) people that are trying to protect this country aren't leaking data?"

So Mr. -- Mr. Rogers asked the question about, you know, how do we know that -- that someone from the White House just can't go turn a switch and begin to listen to their phone conversations?

So General, I think if you could clarify the -- kind of the difference in what the people that are trying to protect this country are doing and what they go through, the rigorous standards. I think it would help, I think, fix this mess for the American people.

ALEXANDER:

Thank you, Congressman.

I think the key -- the key facts here. When we disseminate data, everything that we disseminate and all the queries that are made into the database are 100 percent auditable. So they are audited by not only the analysts who's actually doing the job but the overseers that look and see, did he do that right or she do that right.

In every case that we have seen so far we have not seen one of our analysts willfully do something wrong like what you you just said. That's where disciplinary action would come in.

What I have to overwrite -- underwrite is when somebody makes an honest mistake. These are good people. If they transpose two letters in typing something in, that's an honest mistake. We go back and say, now how can we fix it? The technical controls that you can see that we're adding in help fix that. But is -- it is our intent to do this exactly right.

In that, one of the things that we have is tremendous training programs for our people that they go through. How to protect U.S. persons data? How to interface with the business record FISA? The roles and responsibilities under FAA 702. Everyone, including myself, at NSA has to go through that training to ensure that we do it right.

And we take that very seriously. I believe the best in the world at (ph) terms of protecting our privacy.

And I would just tell you, you know, the other thing that's sometimes confused here is that, "Well, then they're getting everybody else in the world." But our -- our approach is foreign intelligence -- you know, it's the same thing in Europe. We're not interested in -- in -- well, one, we don't have the time. And, two, ours is to protect our country and our allies. I think we do that better than anyone else.

Now, Chris, anything -- if you want to add to that?

INGLIS:

No, I think that's exactly right. When somebody comes to work at NSA, just like elsewhere in the government, they take an oath to the Constitution not to NSA, not to some particular mission but to the Constitution and the entirety of that Constitution. Covers the issues importantly that we're discussing here today: national security and the protection of civil liberties. There's no distinction for us. They're all important.

NUNES:

So I want to -- I want to switch gears a little bit here, General Alexander -- and perhaps this is a good question for Mr. Joyce. But I just find it really odd that right before the Chinese president comes to this country that all of these leaks happen and this guy has fled to -- to Hong Kong, this Snowden. And I'm really concerned that just -- the information that you presented us last week. This is probably gonna be the largest leak in American history -- and there's still probably more to come out. Can you just explain to the American people the seriousness of this leak and the damage -- you said earlier that it's damaged

national security. Can you go into a few of those specifics?

JOYCE:

Very -- no. Really, I can comment very little other than saying it's and ongoing criminal investigation. I can tell you, as we've all seen, these are egregious leaks -- egregious. It has affected -- we are revealing in front of you today methods and techniques. I have told you, the examples I gave you, how important they have been. The first core Al Qaida plot to attack the United States post-9/11 we used one of these programs. Another plot to bomb the New York Stock Exchange, we used these programs. And now here we are talking about this in front of the world. So I think those leaks affect us.

NUNES:

General?

ALEXANDER:

It also -- it also affects our partnership with our allies, because the way it comes out -- and with industry. I mean, it's damaged all of those. Industry's trying to do the right thing, and they're compelled by the courts to do it. And we use this to also protect our allies and our interests abroad.

And so I think the way it's come out and the way it looks is that we're willfully doing something wrong when in fact we're using the courts, Congress and the administration to make sure that everything we do is exactly right. And as Chris noted, we all take an oath to do that, and we take that oath seriously.

NUNES:

And in fact, just in closing here, Mr. Chairman, we know from the Mandiant report that came out that other governments are busy doing this and expanding their cyber warfare techniques. And I just want to say that, you know, it is so vital, as the chairman's pointed out many times, for the folks and the work that you're doing at NSA and all of your folks, how important that is to not only today's security but tomorrow's security.

So thank you for your service, General.

I yield back.

ROGERS:

I -- I would just dispute the fact that other governments do it any -- any way, shape or form close to having any oversight whatsoever of their intelligence gathering programs.

Ms. Sewell?

SEWELL:

Thank you, Mr. Chairman.

I also want to thank all of our witnesses today for your service to this country and for helping to maintain our national security.

I'd like to talk a little bit about the security practices. You've spent a lot of time really explaining to the American people the various levels of complexity in which you have judicial oversight and congressional oversight. How did this happen? How did a relatively low level administrator -- service systems administrator I think you said, General Alexander -- have classified information? And is it an acceptable

risk?

I get that you have 1,000 or so system administrators. It is extremely frightening that you would go through such measures to do the balancing act internally to make sure that we're balancing protection and security and -- and privacy, and yet internally in your own controls, there are system administrators that can go rogue. Is it an acceptable risk? How did it happen? And is there oversight to these system administrators?

ALEXANDER:

Well, there is oversight. What we are now looking at is where that broke down and what happened. And that's gonna be part of the investigation that we're working with the FBI on.

I would just come back to 9/11. One of the key things was we went from the need to know to the need to share. And in this case, what the system administrator had access to is what we'll call the public web forums that NSA operates. And these are the things that talk about how we do our business, not necessarily what's been collected as a results of that; nor does it necessarily give them the insights of the training and the other issues that -- training and certification process and accreditation that our folks go through to actually do this.

ALEXANDER:

So those are in separate programs that require other certificates to get into. Those are all things that we're looking at. You may recall that the intelligence community looked at a new information technology environment that reduces the number of system administrators.

If we could jump to that immediately, I think that would get us a much more secure environment and would reduce this set of problems. It's something that the DNI is leading and that we're supporting, as you know, across the community. I think that is absolutely vital to get to. And there are -- there are mechanisms that we can use there that will help secure this.

Please.

SEWELL:

So the -- to be clear, Snowden did not have the certificates necessarily -- necessary to lead that public forum?

ALEXANDER:

So each -- each set of data that we would have -- and, in this case, let's say the business records, FISA -- you have to have specific certificates -- because this is a cordoned off. So that would be extremely difficult for him -- you'd have to get up to NSA, get into that room.

Others require certificates for you to be working in this area to have that. It -- he would have to get one of those certificates to actually enter that area. Does that make sense? In other words, it's a key.

SEWELL:

Well, I think that -- I would encourage us to figure out a way that we can declassify more information. I thank you for giving us two additional examples of -- of -- of terrorist attacks that we have thwarted because of these programs. But I think that providing us with as much information as you can on FISA courts' opinions -- how -- how that goes -- would help the American public de-mystify what we're

doing here. I think that the examples -- the additional examples that you gave today were great.

But I also am concerned that we have contractors doing -- I get that we cannot -- that there was a move at some point to -- to not have as many government employees, and so we sort of out-sourced it. But given the sensitivity of the information and the access, even for -- for relatively low-level employees, do you see that being a problem? And -- and how do we go about...

ALEXANDER:

So we do have significant concerns in this area. And it is something that we need to look at. The mistakes of one contractor should not tarnish all the contractors because they do great work for our nation, as well. And I think we have to be careful not to throw everyone under the bus because of one person.

But you -- you raised two great points that I think we -- we will look at. One, how do we provide the oversight and compliance? And I talked to our technology director about the two-person control for system administrators to make any change. We are going to implement that. And I think, in terms of what we release to the public, I am for releasing as much as we can. But I want to weigh that with our national security, and I think that's what you expect. That -- that's what the American people...

SEWELL:

Absolutely.

ALEXANDER:

... expect us. So that's where I need to really join that debate on this side to make sure that what we do is exactly right. I think on things like how we minimize data, how we run this program, the -- those kinds of things, I think we can -- we -- we're trying to be -- that's why Chris went through those great details.

I think those are things that the American people should know. Because what they find out is -- shoot, look at the oversight, the compliance, and the training that are people are going through. This is huge. This isn't some rogue operation that a group of guys up at NSA are running. This is something that have oversight by the committees, the courts, the administration in a 100 percent auditable process on a business record FISA.

You know, that's extraordinary oversight. And I think when the American people look at that, they say, "Wow, for less than 300 selectors, that amount of oversight --" and that's what we jointly agreed to do. I think that's tremendous.

SEWELL:

I do too. I -- I -- I applaud the efforts. I just -- I think that, given the nature of this leak, you know, we don't want our efforts to be for naught, if, in fact, what happens is that the -- the leaks get the American people so concerned that they -- we roll back on these programs, and therefore increase our vulnerability as a nation. I think that all of us -- that's not in anyone's best interest.

Going back to sort of the difference between private contractors and government employees, is there a difference in the level of security clearance that...

ALEXANDER:

Same level of security clearance and the same process for securing them.

SEWELL:

OK.

Thank you. I yield back the rest of my time.

ROGERS:

Thank you.

Mr. Westmoreland.

WESTMORELAND:

Thank you, Mr. Chairman.

Mr. Cole, as Mr. Nunes had mentioned about some of the other things that have come out about leaks and so forth, could you -- because my constituents ask me the difference and maybe what the attorney general did in going to the court to -- on the Rosen case saying that he was an unindicted co-conspirator, because that was actually about a leak also. What type of process or internal review did y'all go over before you asked for those phones to be tapped? And, to make it perfectly clear, that was not in a FISA court. Is that correct?

COLE:

Number one, that was not a FISA court. In the Rosen case, there were no phones being tapped. It was just to acquire a couple of e-mails. And there is a very, very robust system. It's set out in regulations that the Department of Justice follows of the kinds of scrubbing and review that must be done before any subpoena like that can be issued.

You have to make sure that you've exhausted all other reasonable avenues of investigation that -- that's done before you even get to the decision about whether or not such a -- a process should be used. You have to make sure that the information you're looking at is very, very tailored and only necessary -- truly necessary to be able to move the investigation forward in a significant way.

There has -- there are restrictions on what can be done with the information. And it goes through a very long process of review from the U.S. attorney's office through the United States attorney him or herself, into the, usually, the criminal division of the Justice Department, through the assistant attorney general of the criminal division, through the deputy attorney general's office and up, ultimately, to the attorney general signing it. It gets a lot of review before that's done under the criteria that we have in our guidelines and our CFR.

WESTMORELAND:

So -- so the DOJ didn't -- because -- (inaudible) a security leak, the DOJ didn't contact the FBI or the NSA, or there was no coordination with that? It was strictly a DOJ criminal investigation?

COLE:

Well, the FBI does criminal investigation with...

WESTMORELAND:

I understand.

COLE:

... the Department of Justice. And they were contacted in that regard. But it was not part of the FISA process. It did not involve the NSA.

WESTMORELAND:

And I think that's what we need to be clear of, is...

COLE:

Correct.

WESTMORELAND:

... that it was absolutely not part of the FISA -- process. And that is a lot more detailed and a lot more scrutinized as far as getting information than what this was. Is that correct?

COLE:

Well, they're both very detailed and very scrutinized processes. They're -- they have different aspects to them. But they're both very unusually, frankly, detailed and scrutinized, both of those processes.

WESTMORELAND:

Thank you.

And, General, going back to what Ms. Sewell had asked about the difference of clearance that you would have with a contractor or a government employee, when you have 1,000 different contractors -- I mean, I know the -- from my experience on having had one of my staff go through a security clearance, it's pretty -- it's a -- it's a pretty detailed operation. And I know that this gentleman had previously, I believe, heard that he had worked for the CIA. Had there been any further clearance given to this individual when he became a contractor after he left the employee of the CIA?

ALEXANDER:

No additional clearance. He had what's needed to work at NSA or one of our facilities, the top secret special intelligence clearance. And that goes through a series of processes and reviews. The director of national intelligence is looking at those processes to make sure that those are all correct. And -- and he stated he's taken that on. We support that objective.

But to work at NSA, whether you're a contract, a government civilian, or a military, you have to have that same level of clearance.

WESTMORELAND:

Does it bother you that this general had only been there for a short period of time? Or is there any oversight or review or whatever of the individuals are that carrying out this work? Is there any type of probation time or -- or anything? Because, you know, it seems that he was there a -- a very short period of time.

ALEXANDER:

So he had worked in a couple of positions. He had just moved into the Booz Allen position in March. But he had worked in a information technology position for the 12 months preceding that at NSA Hawaii. So he'd actually been there 15 months. He moved from one contract to another.

WESTMORELAND:

So would he have been familiar with these programs at his previous job?

ALEXANDER:

Yes. And I believe that's where -- going out on what we call, the public classified web servers that help you understand parts of NSA, that he gained some of the information, and -- and took some of that. I can't go into more detail.

LITT:

Mr. Westmoreland, if I just might...

WESTMORELAND:

Yes?

LITT:

... make one point there? When you say, would he have become familiar with these programs? I think part of the problem that we're having these days is that he wasn't nearly as familiar with these programs as he's portrayed himself to be. And thus -- this is what happens when somebody, you know sees a tiny corner of things and thinks that it gives them insight and viability into the program.

WESTMORELAND:

Thank you. I yield back.

HIMES:

Thank you Mr. Chairman and I too would like to thank the panel for appearing here today and for your service to the country. I think I've told each of you that in my limited time on this committee, I've been heartened by your competence, and by the competence of the agencies in which you work. I'll also add that I've seen nothing in the last week, week and a half to suggest that any of these programs that are being discussed, are operating in any way outside the law. And I would add that the controls that appear to be in place on these programs seem -- seem solid. I'll also say that I don't know that there's any way to do oversight without a posture of skepticism on the part of the overseers.

And so I hope you'll take my observations and questions in that spirit. And I'd like to limit my questions and observations purely to Section 215 and the Verizon disclosures, which quite frankly, trouble me. They trouble me because of the breadth and the scope of the information collection. They trouble me because I think this is historically unprecedented in the extent of the data that is being collected on potentially all American citizens. And the controls which you've laid out for us, notwithstanding, I think new (sic) for this country. We know that when a capability exists, there's a potential for abuse. Mr. Nunes ran through a lot of current issues going back to J. Edgar Hoover bugging the hotel rooms of Martin Luther King, to Nixon, to concerns around the IRS.

If a capability exists, from time to time it will be abused. And one of the things that I'm concerned about is this individual who I -- who's resume would I think make him -- make it unlikely that he would get an unpaid internship in my office, he had access to some of the most sensitive information that we have. And perhaps he could have, or someone like him, could have chosen a different path. Could have accessed phone numbers and -- though we spent a lot of time on the fact that you don't get names, we all know that with a phone number and Google, you can get a name pretty quickly.

He could have chosen to make a point about Congressman Himes making 2:00 am phone calls out of a bar in Washington. Or the CEO of Google making phone calls. Or anything really. Information that we hold to be private. So I guess -- I've got two questions. I guess I direct this one on 215 to Mr. Litt and then Mr. Cole. Where do we draw the line? So in other words, so long as the information is not information to which I have a reasonable expectation of privacy under Maryland v. Smith and under Section 215 powers, where do we draw the line?

Could you, for example have video data? As I walk around Washington my -- I suppose that you could probably reconstruct my day with video that is captured on third-party cameras. Could you keep that in a way that is analogous to what you're doing with phone numbers? And again with all of the careful guards and what not, could you not reconstruct my day because I don't have a reasonable expectation of privacy around -- I know that's a hypothetical, but I'm trying to identify where the line is?

COLE:

Well, I think the -- the real issue here is how it's accessed? What it can be used for? How you can actually...

HIMES:

I -- I -- I'm stipulating that that system, even though we know it's not perfect, I'm stipulating that that system is perfect. And I'm asking, where is the limit as to what you can keep in the tank?

COLE:

I -- I think some of it is a matter for the United States Congress to decide as policy matters, and the legislating that you do surrounding these acts, as to where you're going to draw those lines. Certainly the courts have looked at this and determined that under the statutes we have, there is a relevance requirement, and they're not just saying out of whole cloth you're allowed to gather these things. You have to look at it all together. And they're only saying that you can gather this volume under these circumstances, under these restrictions, with these controls. Without those circumstances and controls and restrictions, the court may well not have approved the orders under 215 to allow that collection to take place.

So you can't separate that out, one from the other and say, just the acquisition, what can we do? Because the acquisition comes together with the restrictions on access.

HIMES:

And if those restrictions and controls are adequate, there's theoretically no restriction on your ability to store information on anything for which I do not have the reasonable expectation for privacy?

COLE:

I'll refer back to NSA...

(CROSSTALK)

HIMES:

Let me...

(CROSSTALK)

HIMES:

... I do have one more question.

(CROSSTALK)

HIMES:

Yeah, this is the conversation -- I do have one more -- much more...

ALEXANDER:

Can I...

HIMES:

... specific question.

ALEXANDER:

... can I hit...

HIMES:

Yeah.

ALEXANDER:

... if I could. I'll ask for more time if I could, because I do think what you've asked is very important. So your question is, could somebody get out and get your phone number and see that you were at a bar last night? The answer is no. Because first in our system, somebody would have had to approve, and there's only 22 people that can approve, a reasonable articulable suspicion on a phone number. So first, that has to get input. Only those phone numbers that are approved could then be queried. And so you have to have one of those 22 break a law. Then you have to have somebody go in and break a law. And the system is 100 percent auditable, so it will be caught.

There is no way to change that. And so on that system, whoever did that would have broken the law. That would be willful. And then that person would be found by the court to be in violation of a court order, and that's much more serious. We have never had that happen.

HIMES:

Yeah. No, I -- I thank you. I appreciate that, and I -- I sort of -- I think it's really important to explore these -- these bright lines about what you can keep and what you can't. Again, I don't see anything about the control systems that are troubling, but I do have one last quick question if the chairman will indulge me in. General, this is I guess for you and it's -- it's something that I asked you in closed session. As we weigh this, because obviously we're weighing security against privacy and what not, as we weigh this, I think it's really important that we understand exactly the national security benefit. And I limit myself to 215 here.

50 episodes. I don't think it's adequate to say that 702 and 215 authorities contributed to our preventing 50 episodes. I think it's really essential that you grade the importance of that contribution. The question I asked you, and -- and you can answer now, or I'd really like to get into this. How many of those 50 episodes would have occurred, but for your ability to use the Section 215 authorities as disclosed in the Verizon situation? How essential, not just contributing to, but how essential are these authorities to

stopping which terrorist attacks?

ALEXANDER:

OK. For clarity over 50. And in 90 percent of those cases FAA 702 contributed, and in 50 percent I believe they were critical. We will send that to the committee.

HIMES:

This is 702 you're talking about?

ALEXANDER:

This is 702.

HIMES:

OK.

ALEXANDER:

Now, shifting to the business record FISA, and I'll do a Mutt and Jeff here, I'm not sure which one I am. There's just over 10 that had a domestic. And the vast majority...

HIMES:

10 of the 50 were section...

ALEXANDER:

Just over 10.

(CROSSTALK)

HIMES:

And how many would you say were critical.

ALEXANDER:

No. No, you're...

HIMES:

I'm sorry.

ALEXANDER:

... let me finish.

HIMES:

Did I get it wrong?

ALEXANDER:

Yeah, you do. Over -- just slightly over 10, and I don't want to pin that number until the community verifies it, so just a little over 10 were a domestic -- had a domestic nexus. And so business records FISA could only apply to those? So, see the ones in other countries, it couldn't apply to because the data is not there and it doesn't come into the U.S. So if we now look at that, the vast majority of those had a contribution by business record FISA. So, I think we have to be careful that you don't try to take the whole world and say, oh well you only did those that were in the United States and only, you know

some large majority of that.

I do think this, going back to 9/11, we didn't have the ability to connect the dots. This adds one more capability to help us do that. And from my perspective, what we're doing here with the civil liberties and privacy oversight, and bringing together, does help connect those dots. Go ahead, Sean?

HIMES:

If I could just -- I -- I'm out of time, but I think this point is really important. If my constituents are representative of the broader American public, they're more concerned frankly with the Section 215 gathering of American data than they are with the foreign data. And so I really hope you'll elucidate for us specifically case by case how many stopped terrorist attacks were those programs, 215, essential to?

JOYCE:

I would just add to General Alexander's comments.

And I -- and I think you asked an almost impossible question to say, how important each dot was.

What I can tell you is, post 9/11 I don't recognize the FBI I came into 26 years ago. Our mission is to stop terrorism, to prevent it. Not after the fact, to prevent it before it happens in the United States. And I can tell you every tool is essential and vital. And the tools as I outlined to you and their uses today have been valuable to stopping some of those plots. You ask, "How can you put the value on an American life?" And I can tell you, it's priceless.

HIMES:

Thank you, Mr. Chairman.

ROGERS:

(OFF-MIKE)

BACHMANN:

Thank you, Mr. Chair, for holding this important hearing today.

I just have a series of short questions. My first one is, you had mentioned earlier in your testimony that data must be destroyed within five years of acquisition. I believe that's in section 215 phone records. Is that -- that's true, within five years?

INGLIS:

That is true. It's destroyed when it reaches five years of age.

BACHMANN:

And how long do the phone companies on their own maintain data?

INGLIS:

That varies. They don't hold that data for the benefit of the government. They hold that for their own business internal processes. I don't know the specifics. I know that it is variable. I think that it ranges from six to 18 months and the data that they hold is, again, useful for their purposes, not necessarily the government's.

BACHMANN:

So then my question is, did the FISA orders give the United States companies a choice in whether to participate in the NSA business records or in the PRISM programs? Were these -- was this voluntarily -- voluntary compliance on the part of these companies?

INGLIS:

No, these are court orders that require their compliance with the terms of the court order.

BACHMANN:

So let me just for the record state, is NSA spying today or have you spied on American citizens?

INGLIS:

We -- we do not target U.S. persons anywhere in the world without a specific court warrant.

BACHMANN:

And does the NSA listen to the phone calls of American citizens?

INGLIS:

We do not target or listen to the telephone calls of U.S. persons under that targeting without a specific court warrant.

BACHMANN:

Does the NSA read the e-mails of American citizens?

INGLIS:

Same answer, ma'am.

BACHMANN:

Does the NSA read the text messages of American citizens?

INGLIS:

Again, we do not target the content of U.S.-person communications without a specific warrant anywhere on the earth.

BACHMANN:

Has the NSA ever tracked any political enemies of the administration, whether it's a Republican administration or Democrat administration? Have either of the administrations -- you said you're 100 percent auditable, so you would know the answer to this question -- have you ever tracked the political enemies of an administration?

INGLIS:

In my time at NSA, no, ma'am.

BACHMANN:

Does the government keep the video data, like Mr. Himes had just questioned? Does the government have a database with video data in it, tracking movements of the American people?

INGLIS:

No, ma'am.

(CROSSTALK)

BACHMANN:

I'm sorry. That's not -- the microphone isn't on.

INGLIS:

NSA does not hold such data.

ALEXANDER:

Yeah, and we don't know of any data -- anybody that does. So I think those are held, as you see from Boston, by individual shop owners and (inaudible).

BACHMANN:

But -- but does the federal government have a database with video data in it tracking the whereabouts of the American people?

JOYCE:

The FBI does not have such a database, nor am I aware of one.

BACHMANN:

Do we -- does the American government have a database that has the GPS location whereabouts of Americans, whether it's by our cell phones or by any other tracking device? Is there a known database?

INGLIS:

NSA does not hold such a database.

BACHMANN:

Does the NSA have a database that you maintain that holds the content of Americans' phone calls? Do you have recordings of all of our calls? So if we're making phone calls, is there a national database that has the content of our calls?

ALEXANDER:

We're not allowed to do that, nor do we do that, unless we have a court order to do that. And it would be only in specific cases and almost always that would be an FBI lead, not ours.

BACHMANN:

So do we maintain a database of all of the e-mails that have ever been sent by the American people?

ALEXANDER:

No. No, we do not.

BACHMANN:

Do we -- is there a database from our government that maintains a database of the text messages of all Americans?

ALEXANDER:

No -- none that I know of, and none at NSA.

BACHMANN:

And so I think what you have told this committee is that the problem is not with the NSA, that is trying to keep the American people safe. You've told us that you have 100 percent auditable system that has oversight both from the court and from Congress.

It seems to me that the problem here is that of an individual who worked within the system, who broke laws, and who chose to declassify highly sensitive classified information. It seems to me that's where our focus should be, on how there could be a betrayal of trust and how a traitor could do something like this to the American people. It seems to me that's where our focus must be and how we can prevent something like that from ever happening again.

Let me ask your opinion: How damaging is this to the national security of the American people that this trust was violated?

ALEXANDER:

I think it was irreversible and significant damage to this nation.

BACHMAN:

Has this helped America's enemies?

ALEXANDER:

I believe it has. And I believe it will hurt us and our allies.

BACHMANN:

I yield back, Mr. Chair.

ROONEY:

Thank you, Mr. Chairman.

I want to thank the panel.

You know, one of the negatives about being so low on the totem pole up here is basically all the questions that I wanted to address have been asked.

And I think I'm really proud of this committee because on both sides of the aisle, a lot of the questions were very poignant. And I hope that the American people and those that are in the room have learned a lot about what happened here and learned a lot about the people on the panel.

I can say specifically, General Alexander, my time on the Intelligence Committee, I have more respect for you. And I'm glad that you're the one up there testifying so the American people can see despite what they're -- what's being portrayed and the suspicions that are out there, that there is nobody better to articulate what happened and what we're trying to do than yourself.

So I want to thank you for that.

We -- we -- I'll ask a couple basic questions that I think that might help clear some things up.

Mr. Cole, you talked about how the -- the Fourth Amendment isn't applicable under the business records exception and the Patriot Act Section 215, applicable case law, Maryland v. Smith, et cetera.

And then we heard about how to -- to be able to look at the data under 215, there has to be very specific suspicion that is presented to a court, and that court is not a rubber stamp in allowing us to basically look at metadata which is strictly phone records.

One of, I think, problems that people have out there is that it was such a large number of phone numbers. And when you testify, when everybody testifies, that it's very specific and only a limited number of people are able to -- to basically articulate who we should be looking at and then you hear this number, millions, from Verizon, can you -- can you help clear that up?

COLE:

Certainly. First of all we -- as we said, we don't give the reasonable suspicion to the court ahead of time. They set out the standards for us to use.

But the analogy, and I've heard it used several times is, if you're looking for a needle in the haystack, you have to get the haystack first. And that's why we have the ability under the court order to acquire -- and the key word here is acquire -- all of that data.

We don't get to use all of that data necessarily. That is the next step, which is you have to be able to determine that there is reasonable, articulable suspicion to actually use that data.

So if we want to find that there is a phone number that we believe is connected with terrorist organizations and terrorist activity, we need to have the rest of the haystack, all the other numbers, to find out which ones it was in contact with.

And, as you heard Mr. Inglis say, it's a very limited number of times that we make those queries because we do have standards that have to be met before we can even make use of that data. So while it sits there, it is used sparingly.

ROONEY:

Did you or anybody that you know at the NSA break the law in trying to obtain this information?

COLE:

I am aware of nobody who has broken the law at the NSA in obtaining the information in the lawful sense. There's other issues that we have with the leaks that have gone on here.

ROONEY:

And maybe this question is for General Alexander: Based on everything that we've heard today, do you see any problems with either 702 or 215 that you think should be changed by this body?

ALEXANDER:

Not right now. But this is something that we have agreed that we would look at, especially the structure of how we do it.

I think Congressman Schiff brought up some key points, and we are looking at all of those. And what we have to bring back to you is the agility, how we do it in the oversight, is there other ways that we can do this.

But at the end of the day, we need these tools and we just got to figure out the right way to do it or the next step from my perspective, having the court, this body of Congress and the administration do

oversight.

I think if the American people were to step through it, they would agree that what we're doing is exactly the right way.

ALEXANDER:

So those are the steps that we will absolutely they'll go back and -- and look at the entire architecture and that's a commitment that FBI and NSA has made to the administration and to this committee.

ROONEY:

Final question, Mr. Joyce, what's next for Mr. Snowden we can expect?

JOYCE:

Justice.

ROONEY:

I yield back, Mr. Chairman. Thank you.

(CROSSTALK)

POMPEO:

Great. Thank you, Mr. Chairman.

Thank you all for being here today. You know, this has been -- this has been a great hearing. I think the American people will have gotten a chance to hear from folks who are actually executing this program in an important way, and they'll have a choice whether to believe Mr. Inglis and General Alexander or a felon who fled to communist China.

For me, there's an easy answer to that.

There are those who talk about the war on terror winding down, they say we're toward the end of this, these programs were created post-9/11 to counter the terrorist threat, but for the soldiers fighting overseas and our allies and for us in the States.

General Alexander, Mr. Joyce, do you think these programs are just as much needed today as they were in the immediate aftermath of 9/11?

ALEXANDER:

I do.

JOYCE:

I do, too. And I would just add, I think the environment has become more challenging. And I think the more tools you have to be able to fight terrorism, the more we're gonna be able to protect the American people.

POMPEO:

Thank you.

We've talked a lot about the statutory basis for Section 215 and Section 702. We've talked a lot on all the process that goes with them. And I want to spend just a minute talking about the constitutional

boundaries and where they are.

We've got FISA court judges, Article 3. Mr. Litt, these are just plain old Article 3 judges, in the sense of life time tenure, nominated by a president, confirmed by the United States Senate. They have the same power, restrictions and authority as all Article 3 judges do. Is that correct?

LITT:

Yes, that's correct.

POMPEO:

We have Article 2 before us here today and we've got Article 1 oversight taking place this morning.

I want to talk about Article 1's involvement. There have been some members who talked about the fact that they didn't know about these programs. General Alexander or maybe Mr. Inglis, can you talk about the briefings that you've provided for members of Congress, both recently and as this set of laws was developed -- set of laws were developed?

INGLIS:

So 702 was recently reauthorized at the end of 2012. In the runup to that, NSA in the companionship with the Department of Justice, FBI, the DNI, made a series of presentations across the Hill some number of times and talked in very specific details at the classified level about the setup of those programs, the controls on those programs and the success of those programs.

The reauthorization of Section 215 of the Patriot Act came earlier than that, but there was a similar set of briefings along those lines.

At the same time, we welcome and continue to welcome any and all Congress persons or senators to come to NSA or we can come to you and at the classified level brief any and all details, That's a standing offer. And some number have, in fact taken us up on that offer.

POMPEO:

Do you have something to add, General?

ALEXANDER:

That's exactly right. In fact, anyplace, anytime we can help, we will do it.

POMPEO:

Good. I appreciate that. I've been on the committee only a short time. I learned about these programs actually before I came on the committee, so I know that members outside of this committee also had access to the information. And I think that's incredibly important.

As -- as committee oversight members, that's one thing, but I think it's important that all the members of Congress understand the scope of these programs. And I appreciate the fact that you've continued to offer that assistance for all of us.

A couple of just clean-up details, going last. I want to make sure I have this right.

General Alexander, from the data under Section 215 that's collected, can you -- can you figure out the location of the person who made a particular phone call?

ALEXANDER:

Not beyond the area code.

POMPEO:

Do you have any information about the signal strength or tower direction? I've seen articles that talk about you having this information. I want to...

(CROSSTALK)

ALEXANDER:

No, we don't.

POMPEO:

... we've got that right.

ALEXANDER:

We don't have that in the database.

POMPEO:

And then, lastly, Mr. Litt, you made a reference to Section 702. You talked about it being a restriction on Article 230, not an expansion. That is, Article 2, the presidents of both parties believed they had the -- the powers that are being exercised under Section 702 long before that statutory authority was granted.

So is it the case that you view Section 702 as a control and a restriction on Article 2?

LITT:

Yes.

POMPEO:

Great.

Mr. Chairman, I yield back.

(OFF-MIKE)

KING:

Thank you, Mr. Chairman. I'll make this brief.

I want to first of all thank all witnesses for their testimony, for their service, and for all you've done to strengthen and maintain this program.

My question, General Alexander, is -- is to you and also perhaps to Mr. Joyce,

Several times in your testimony you referenced 9/11 and how -- and I recall after September 11th there was a -- was a loud challenge to the intelligence community to do a better job of connecting the dots, be more aggressive, be -- you know, be more forward thinking, try to anticipate what's going to happen, think outside the box, all those cliches we heard at the time.

And as I see it, this is a very legitimate and legal response to that request.

I would ask you, General Alexander, or you, Mr. Joyce, I believe referenced the case, after September

11th where there was a phone interception from Yemen which enabled you to foil the New York Stock Exchange plot,

It's also my understanding that prior to 9/11, there was phone messages from Yemen which you did not have the capacity to follow through on which perhaps could have prevented the 9/11 attack.

Could either General Alexander or Mr. Joyce or both of you explain how the attack could have been prevented? Or if you believe it could have been prevented?

JOYCE:

I don't know, Congressman, if the attack could have been prevented. What I can tell you is that is a tool that was not available to us at the time of 9/11. So when there was actually a call made from a known terrorist in Yemen to Khalid Mihdhar in San Diego, we did not have that tool or capability to track that call.

Now, things may have been different, and we will never know that, unfortunately.

So that is the tool that we're talking about today that we did not have at the time of 9/11.

Moving forward, as you mentioned about the -- the stock exchange, here we have a similar thing except this was under, again, the 702 program, where NSA tipped to us that a known extremist in Yemen was talking or conversing with an individual inside the United States, we later identified as Khalid Ouazzani.

And then we were able to go up on our legal authorities here in the United States on Ouazzani, who was in Kansas City and were able to identify two additional co-conspirators.

We found through electronic surveillance they were actually in the initial stages of plotting to bomb the New York Stock Exchange.

So, as -- to really summarize, as I mentioned before, all of these tools are important.

And as Congressman Schiff mentioned, we should have this dialogue. We should all be looking for ways, as you said, thinking outside the box of how to do our business.

But I sit here before you today humbly and say that these tools have helped us.

KING:

General?

ALEXANDER:

If I could, I think on Mihdhar case, Mihdhar was the terrorist -- the A.Q. terrorist from the 9/11 plot in California that was actually on American Airlines Flight 77 that crashed into the Pentagon -- what -- what we don't know going back in time is the phone call between Yemen and there, if we would have had the reasonable, articulable suspicion standard, so we'd have to look at that.

But assuming that we did, if we had the database that we have now with the business records FISA and we searched on that Yemen number and saw it was talking to someone this California, we could have then tipped that to the FBI.

Another step, and this an assumption, but let me play this out because we will never be able to go all the way back and redo all the figures from 9/11, but this is why some of these programs were put in was to

help that.

Ideally going from Mihdhar, we would have been able to find the other teams, the other three teams in the United States and/or one in Germany or some other place.

So the ability to use the metadata from the business record FISA would have allowed us, we believe, to see some.

Now, so it's hypothetical. There are a lot of conditions that we can put -- that we could put on there. You'd have to have this right. You'd have to have the RAS right.

But we didn't have that ability. We couldn't connect the dots because we didn't have the dots.

And so, I think what we've got here is that one additional capability, one more tool to help us work together as a team to stop future attacks. And as -- as Sean has laid out, you know, when you look at this, you know, the New York City -- two and others, I think from my perspective, you know, those would have been significant events for our nation. And so, I think what we've jointly done with Congress is helped set this program up correctly.

KING:

I'll just close, General, by saying in your opening statement you said that you'd rather be testifying here today on this issue rather than explaining why another 9/11 happened.

So I want to thank you for your service in preventing another 9/11 and there's the Zazi case. And I know some -- you're very close with your knowledge of that. And I want to thank all of you for the effort that was done to prevent that attack.

Mr. Chairman, I yield back.

ROGERS:

Just a couple of clarifying things here to -- to wrap it up.

Mr. Joyce, you've been in the FBI for 26 years. You've conducted criminal investigations as well.

Sometimes you get a simple tip that leads to a broader investigation. Is that correct?

JOYCE:

That is correct, Chairman.

ROGERS:

And so, without that initial tip, you might not have found the other very weighty evidence that happened subsequent to that tip. Is that correct?

JOYCE:

Absolutely.

ROGERS:

So, in the case of -- of Malalin (ph) in 2007, the very fact that under the business 215 records, there was a simple tip that was, we have someone that is known with ties to Al Qaida's east African network calling a phone number in San Diego. That's really all you got, was a phone number in San Diego. Is that correct?

JOYCE:

That is correct.

ROGERS:

And -- and according to -- in the unclassified report that tip ultimately led to the FBI's opening of a full investigation that resulted in the February 2013 conviction. Is that correct?

JOYCE:

Yes, it is, Chairman.

ROGERS:

So without that first tip, you would have had -- you -- you weren't up on his electronics communications. You didn't really -- you were not -- he was not a subject of any investigation prior to that tip from the National Security Agency.

JOYCE:

No, actually, he was the subject to a prior investigation...

ROGERS:

That was closed.

JOYCE:

... several years earlier that was closed...

ROGERS:

Right.

JOYCE:

... because we could not find any connection to terrorism.

ROGERS:

Right.

JOYCE:

And then, if we did not have the tip from NSA, we would not have been able to reopen...

ROGERS:

Reopen the case. But at the time, you weren't investigating him?

JOYCE:

Absolutely not. It was based on...

(CROSSTALK)

ROGERS:

Right, and when they -- when they dipped that number into the -- to the business records, the preserved business records from the court order -- they dipped a phone number in, and a phone number came out in San Diego. Did you know who that person was when they gave you that phone number?

JOYCE:

No, we did not. So we had to serve legal process to identify that subscriber and then corroborate it. And then we later went up on electronic surveillance with an order through the FISC.

ROGERS:

And -- and when you went up on the electronic surveillance, you used a court order, a warrant...

JOYCE:

That is correct.

ROGERS:

... a subpoena? What did you use?

JOYCE:

We used a FISA court order.

ROGERS:

All right. So you had to go back. You had to prove a standard of probable cause to go up on this individual's phone number. Is that correct?

JOYCE:

That's right. And as been mentioned, hopefully several times today, anyone inside the United States, a U.S. person, whether they're inside or outside, we need a specific court order regarding that person.

ROGERS:

All right.

And Mr. Cole, I just -- just for purposes of explanation, if you were going to have a -- an FBI agent came to you for an order to preserve business records, do they need a court order? Do they need a warrant for that in a criminal investigation?

COLE:

No, they do not. You can just get a grand jury's subpoena, and, separate from preserving it, you can acquire them with a grand jury subpoena. And you don't need to go to a court to do that.

ROGERS:

Right, so that is a lower-legal standard in order to obtain information on a U.S. citizen on a criminal matter.

COLE:

That's correct, Mr. Chairman.

ROGERS:

So the -- when we -- and I think this is an important point to make. When we -- the system is set up on this foreign collection -- and I argue we need this high standard because it is in a classified -- or used to be in a classified setting -- you need to have this high standard. So can you describe the difference?

If I were going to do a criminal investigation -- getting the same amount of information the -- the legal

standard would be much lower if I were working an embezzlement case in Chicago than trying to catch a counter-terrorist -- counter -- excuse me, a terrorist operating overseas trying to get back into the United States to conduct a plot.

COLE:

Some of the standards might be similar, but the process that you have to go through is much greater in the FISA context. You actually have to go to a -- a court, the FISA court ahead of time and set out facts that will explain to the court why this information is relevant to the investigation that you're doing, why it's a limited type of investigation that is allowed to be done under the statute and under the rules. And then the court has to approve that ahead of time, along with all of the rules and restrictions about how you can use it, how you can access it, what you can do with it, and who you can disseminate it to.

There is a much different program that goes on in a normal grand jury -- situation. You have restrictions on who you can disseminate to under secrecy grounds, but even those are much broader than they would be under the FISA grounds.

ROGERS:

Right.

COLE:

And you don't need a court ahead of time.

ROGERS:

So -- so, in total, this is a much more overseen -- and, by the way, on a criminal embezzlement case in Chicago, you wouldn't brief that to Congress, would you?

COLE:

No, we would not, not as a normal course.

ROGERS:

Yeah, and so you have a whole nother layer of legislative oversight on this particular program. And, again, I argue the necessity of that because it is a -- as I said, used to be a classified program of which you additional oversight. You want members of the legislature making sure we're (ph) on track that you don't necessarily need in a criminal matter domestically.

COLE:

That's correct. In a normal criminal embezzlement case in Chicago, you would have the FBI and the Justice Department involved. And that's about it.

ROGERS:

Right.

COLE:

In this, you've got the National Security -- Agency. You've got the ODNI. You've got the inspectors general. You've got the Department of Justice. You have the court monitoring what you're doing, if there's any mistakes that were made. You have Congress being briefed on a regular basis. There is an enormous amount of oversight in this compared to a grand jury situation. Yet the records that can be

obtained are of the same kind.

ROGERS:

Right, thanks. And I just want a couple of clarifying questions.

Mr. Joyce, if you will, does China have an -- an adversarial intelligence service directed at the United States?

JOYCE:

Yes, they do.

ROGERS:

Do they perform economic espionage activities targeted at U.S. companies in the United States?

JOYCE:

Yes, they do.

ROGERS:

Do they conduct espionage activities toward military and intelligent services, both here and abroad, that belong to the United States of America?

JOYCE:

Yes, they do.

ROGERS:

Do they target policy makers and decision makers, Department of State and other -- other policy makers that might engage in foreign affairs when it comes to the United States?

JOYCE:

Yes.

ROGERS:

Would you -- how would you rate them as an adversarial intelligence service given the other intelligence services that we know are adversarial, the Russians, the Iranians, the others?

JOYCE:

They are one of our top adversaries.

ROGERS:

Yeah. And you have had a string of successes recently in prosecutions for Chinese espionage activities in the United States. Is that correct?

JOYCE:

That is correct.

ROGERS:

And so, that has been both economic, and, if I understand it, as well as the military efforts. So they've been very aggressive in their espionage activities toward the United States. Is it -- would you -- is that a

fair assessment?

JOYCE:

I think they have been very aggressive against United States interests.

ROGERS:

General Alexander, do they -- how would you describe, in an unclassified way, the Chinese cyber efforts for both espionage and their military capability to conduct disruptive attacks toward the United States?

ALEXANDER:

Very carefully.

(LAUGHTER)

With a lot of legal oversight. I -- I think one of the things that -- you know, it's public knowledge out there about the cyber activities that we're seeing. But I also think that what's missing, perhaps, in this conversation with the Chinese is what's -- what's acceptable practices here. And I think the president has started some of that in the discussions with the -- the new president of China.

And I think that's some of the stuff that we actually have to have. This need not be an adversarial relationship. I think our country does a lot of business with China, and we need to look at, how can we improve the relations with China in such a way that both our countries benefit? Because we can. And I think that's good for everybody.

What concerns me is now this program and what we're talking about with China, as got -- I think we've got to solve this issue with China and then look at ways to move -- to move forward. And I think we do have to have that discussion on cyber. What is -- what are the right standards, have that discussion both privately and publicly. And it's not just our country. It's all the countries of the world, as well as China.

ROGERS:

All right, and I -- I appreciate you drawing the line, but would you say that China engages in economic -- cyber economic espionage against intellectual property to steal intellectual property in the United States?

ALEXANDER:

Yes.

ROGERS:

Would you argue that they engage in cyber activities to steal both military and intelligence secrets of the United States?

ALEXANDER:

Yes.

ROGERS:

I -- I just -- I think this is important that we put it in context for several things that I think Americans want to know about the relationship between Mr. Snowden and -- and where he finds home today, and that we know that we're doing a full investigation into possible connections with any nation state who

might take advantage of this activity.

And the one thing I disagree with Mr. Litt today, that they haven't seen anything of any changes. And I would dispute that based on information I've seen recently and would ask anyone to comment. Do you believe that Al Qaida elements have -- have just historically, when they've been -- when issues have been disclosed, changed the way they operate to target both soldiers abroad in their terrorist- plotting activities, movements, financing, weaponization, and training.

LITT:

To -- to be clear, what I -- what I intended to say -- and if I wasn't clear, I apologize -- was we know that they've seen this. We know they've commented on it. What we don't know yet is over the long term what impact it's going to have on our collection capabilities. But you're absolutely right. We know they watch us. And they -- they -- they modify their behavior based on what they learn.

ROGERS:

And -- and we also know that in some cases in certain countries they have modified their behavior, including the way they target U.S. troops based on certain understandings of communications. Is that correct?

LITT:

I think that's -- that's correct.

ROGERS:

I'll guarantee it's absolutely correct. And that's what's so concerning about this.

I do appreciate your being here. I know how difficult it is to come and talk.

General, did you want to say something before...

(CROSSTALK)

ALEXANDER:

Yeah, I -- I wanted to say, if I could, just a couple things, because they didn't come up in -- in this testimony. But, first, thanks to this committee, the administration and others, in the summer of 2009 we set up the director -- Directorate of Compliance. Put some of our best people in it to ensure that what we're doing is exactly right. And this committee was instrumental in helping us set that up. So that's one point.

When we talk about oversight and compliance, people think it's just once in a while, but there was rigorous actions by you and this entire committee to set that up.

The second is, in the open press there's this discussion about pattern analysis -- they're out there doing pattern analysis on this. That is absolutely incorrect. We are not authorized to go into the data, nor are we data mining or doing anything with the data other than those queries that we discuss, period. We're not authorized to do it. We aren't doing it. There are no automated processes running in the background pulling together data trying to figure out networks.

The only time you can do pattern analysis is, once you start the query on that query and where you go forward. You can't go in and try to bring up -- you know, I have four daughters and 15 grandchildren. I

can't supervise them with this database. It is not authorized, and our folks do not do it.

And so that's some of the oversight and compliance you and the rest of the Oversight Committee see, but I think it's important for the American people to know that it's limited. In this case, for 2012, less than 300 selectors were looked at, and they had an impact in helping us prevent potential terrorist attacks, they contributed. And I think when you look at that and you -- you balance those two, that's pretty good.

ROGERS:

And I do appreciate it. And I want to commend -- the folks from the NSA have always -- we've never had to issue a subpoena. All that information has always -- readily provided. You meet with us regularly. We have staff and investigators at the NSA frequently. We have an open dialogue when problems happen; we do deal with them in a classified way, in -- in a way I think that Americans would be proud that their elected representatives deal with issues.

And I'm not saying that there are some hidden issues out there; there are not.

I know this has been difficult to come and talk about very sensitive things in a public way. In order to preserve your good work and the work on behalf of all the patriots working to defend America, I still believe it was important to have a meeting where we could at least, in some way, discuss and reassure the level of oversight and redundancy of oversight on a program that we all recognize needed an extra care and attention and lots of sets of eyes. I hope today in this hearing that we've been able to do that.

I do believe that America has the responsibility to keep some things secret as we serve to protect this country. And I think you all do that well. And the darndest thing is that we may have found that it is easier for a systems analyst -- or a systems administrator to steal the information than it is for us to access the program in order to prevent a terrorist attack in the United States. And we'll be working more on those issues.

And we have had great dialogue about what's coming on some other oversight issues.

Again, thank you very, very much. Thank you all for your service. And I wish you all well today.

List of Panel Members and Witnesses PANEL MEMBERS:

REP. MIKE ROGERS, R-MICH. CHAIRMAN

REP. MAC THORNBERRY, R-TEXAS

REP. JEFF MILLER, R-FLA.

REP. K. MICHAEL CONAWAY, R-TEXAS

REP. PETER T. KING, R-N.Y.

REP. FRANK A. LOBIONDO, R-N.J.

REP. DEVIN NUNES, R-CALIF.

REP. LYNN WESTMORELAND, R-GA.

REP. MICHELE BACHMANN, R-MINN.

REP. JOE HECK, R-NEV.

REP. TOM ROONEY, R-FLA.

REP. MIKE POMPEO, R-KAN.

REP. JOHN A. BOEHNER, R-OHIO EX OFFICIO

REP. C.A. DUTCH RUPPERSBERGER, D-MD. RANKING MEMBER

REP. MIKE THOMPSON, D-CALIF.

REP. JAN SCHAKOWSKY, D-ILL.

REP. JIM LANGEVIN, D-R.I.

REP. ADAM B. SCHIFF, D-CALIF.

REP. LUIS V. GUTIERREZ, D-ILL.

REP. JIM HIMES, D-CONN.

REP. ED PASTOR, D-ARIZ.

REP. TERRI A. SEWELL, D-ALA.

REP. NANCY PELOSI, D-CALIF. EX OFFICIO

WITNESSES:

GENERAL KEITH ALEXANDER (USA), DIRECTOR, NATIONAL SECURITY AGENCY

CHRIS INGLIS DEPUTY DIRECTOR, NATIONAL SECURITY AGENCY

JAMES COLE, DEPUTY ATTORNEY GENERAL

SEAN JOYCE, DEPUTY DIRECTOR, FEDERAL BUREAU OF INVESTIGATION

ROBERT LITT, GENERAL COUNSEL, OFFICE OF THE DIRECTOR OF NATIONAL INTELLIGENCE GENERAL COUNSEL