PRESS BRIEFING: Mr. John DeLong, NSA Director of Compliance

Moderator: Ms. Judith Emmel, NSA Director, Strategic Communications

August 16, 2013

Coordinator: Welcome and thank you for standing by. At this time all participants are in a listen only mode until the question and answer session of the call. To ask a question during that time please press star then 1. Today's conference is being recorded, if you have any objections, you may disconnect at this time. Now I'd like to turn over the meeting to Judi Emmel, you may begin.

Judith Emmel: Good afternoon everyone. Thank you very much for joining us today, this is a very important session for us. We are very much looking forward to addressing a lot of the inaccuracies that are out there in today's reporting about compliance in NSA and our compliance program here today.

We will be taping this and invite others to -- but we ask people to use pad and pen. We will be interviewing with our NSA Director of Compliance Mr. John DeLong. And I'm going to spell that for you now in case anybody has to drop out. John - J-O-H-N DeLong - D-E-L-O-N-G. He is NSA's Director of Compliance and works directly for General Alexander in that capacity.

Our ground rules today will be on the record. We will be having a 45 minute opportunity here to talk with John. And he'll start with some opening comments and then we'll go to some question and answer.

With that, I'll turn it over to Mr. DeLong.

John DeLong: Great. Good afternoon this is John DeLong, director of compliance at NSA. Been a busy day, I do want to cover a few things first. I think the most important thing for everyone to understand is that no one at NSA thinks a mistake is okay. That's really got to get out there.

We have an internal oversight and compliance program for the purpose of -- of multiple purposes. Preventing mistakes and then when mistakes do occur, to detect them and correct them at the earliest point possible.

The document that was listed in the article is an internal document at NSA. It's something we do each and every quarter, we - there's other documents that we do to understand where mistakes do occur. To correct them and then to take remedial action both for that specific mistake and for other areas that we know we know need to improve.

What's not reported each and every day are the number of times that NSA's activities are consistent with law and policy and I think that context is very important.

Let me just give you some statistics. So in the document that was in the article, there were reported, let's just say about a hundred data base query incidents. So that's an analyst making a query, looking for information that's already been collected, that's in a database, to answer some need that's responsive to a foreign intelligence requirement.

Per month, we do about 20 million queries. So if you take that number and you make that the denominator and you take the numerator of about a hundred queries. You get to essentially .0005% error rate. We're talking parts per million. And I think it's important for folks to understand that.

Now we recognize that that's a lot of activity. And there's a lot of discussions about the activity that's occurring and we understand that. But it's important for people to understand that no one at NSA thinks a mistake is okay. But we - those kinds of reports are designed and generated directly to make sure we understand when mistakes do occur and to document our corrective actions and to document our remedial actions.

Those incidents are then reported internally within NSA, to a variety of folks, and organizations, the director, etc., especially our Office of Inspector General and our Office of General Counsel. And then they, as part of their duties report those incidents externally. So I want to make sure folks understand that.

What was in the article is actually an internal document. I think some of the confusion that's out there is that's not a document, that's a document that forms the basis, right, of reports that come from the office of Inspector General, the Office of our General Counsel, that go to a variety of sources through a variety of means.

So, to the Department of Defense as part of the regular quarterly reporting; to the Department of Justice, if there is a FISA incident or an incident under FISC approval and if you look in the document you'll see that they're broken out by that.

To the Office of the Director of National Intelligence. Through a - to Congress then, to a variety of means. Both immediate at times and then periodic reporting, quarterly, semi-annually, annually. Each of those reports has a different form and function and it's typically dictated by what our different overseers the way they like to see information. So I think there's some confusion out there over why, for example, certain overseers have not seen this document.

And again, this is a document that creates a variety of reports where they see. A lot of the information that's in this document goes in different forms to multiple overseers. So a lot of them have seen the information, it's just in a different form. And the fast pace we're moving today, where folks are having to generate comments on what they have and have not seen. I think we're confusing, "Have you seen a document?" with, "Have you seen information that's in the document?" So I want to hit that.

I do think in a lot of the headlines and other things, there's people talking about privacy violations or abuses or willful or violations, right, it is important for people to understand, NSA has a zero tolerance policy for willful misconduct. Zero. That's our tolerance, it's very simple.

Right, we do realize mistakes do occur. We detect them, as early as we can. We correct them, right. None of the mistakes, the incidents that were in the document released were willful. Right, it doesn't mean that we have any desire to have any mistakes; it doesn't mean we think a mistake is okay.

But we recognize that we are an organization that's charged with a very important foreign intelligence mission. And that, for example, you know, 20 million database queries a month, take that as a denominator, you take the number that you see in there and you make that as a numerator.

Right, there's tens of thousands of people at NSA, they're not all doing this activity. There's some that keep the lights on and provide us, right, you know, make sure we have food, etcetera. Those are critical but, you know, think about over ten thousand people and think about if each one of them were to make one mistake a quarter, alright, that's a totally different number and a

different perspective on it. So, I really want to make sure people understand that.

The additional point that is very important as well is a lot of people are talking about every one of these mistakes sort of on the same spectrum of a privacy violation, a direct violation of a US person. It's important to understand that a number of these incidents involve foreign nationals, non US persons.

Alright, so for example, there are incidents where a non US person that's overseas is the subject of NSA collections. That person travels into the United States, right. There's a category you'll see there called roamers. I realize that, you know, there's a bit of need to explain why and how that occurs. But that occurs without us knowing, and what we do is detect as soon as we can, right, make sure we take corrective action to stop the collection.

Right, as appropriate, we will remove that information from our databases. Right, especially such as an analyst may in fact and often in fact never even sees the information that was collected while a person was inside the United States.

There's different timing things that go on there. So, you know, there's a spectrum of how soon we can detect and correct but this gets me to really my almost second to last point which is, you can think of NSA's activity as an assembly line. Think of it as a series of steps that occur to generate the intelligence and information that our nation needs.

The procedures that NSA operates under in the, in the specific - they are called minimization procedures, in the more generic term you might call them privacy protecting procedures. They regulate every aspect of our activity from what we can collect to where we can collect to what we can do when we

process and retain the information and how long we can retain it. What type of queries are acceptable to go into that information. And then even what we can share.

So those are generally known as attorney general approved minimization procedures. Probably more easy to think of them as privacy protecting procedures.

Those procedures contemplate from day one the idea - really two concepts. One is that even as we are collecting on a non US person who is overseas they may in fact communicate with another person overseas who happens to be a US person. Or they might talk about a US person.

The procedures, by design, right, are designed with US person privacy in mind. They are designed to minimize out, that's not a term that sort of resonates well, but they're designed to reduce the impact on US person privacy at each and every phase of that, of our assembly line.

In the context of the documents that were in the article, it's very important for people to understand that what we are detecting and correcting in many cases are a mistake that occurs at one step of that assembly line. So for example we might have an incident where we collected something mistakenly. The goal then is to detect and correct that before that information is available to an analyst or before that information can then be shared, right?

Or if an improper query is made, we're going to detect and correct that and in some cases no result of that query will be used for any purpose, right, it will not be shared outside the building.

So I want to make sure people understand that these incidents are and these mistakes occur at phases of that cycle and the procedures themselves contemplate that it will be a phased process and the way we approach oversight and compliance as well is to detect and correct within each of those phases such that mistakes do not propagate through the system right.

You can look at that document. We look at that document. We do it each and every day. It's not just that document, but other trend assessments, other things we work on, right. The goal is always to make sure we are minimizing out, right, the number of incidents in the first place, the number of mistakes but those that we, that do occur, we will detect and correct them.

Right, and to absolutely in first instance be sure that they do not percolate through. Right, no, we have a number of technical safeguards, sometimes we have the law and the policies and procedures baked into the technology itself.

We also coupled out with training, mandatory training, testing, periodic training. You know, additional awareness campaigns, if in fact somebody makes a mistake in a query and we look at it and we say, we will go back at that time to that analyst and say, "Let's make sure we understand and let's make sure we maybe go over the training again," right.

And again, back to my last thing, and I'll stop here. No one at NSA thinks a mistake is okay, right, it's part of our culture. It's what happens to every employee that walks in here. They take an oath to the constitution, right. They learn and they understand that they have intelligence oversight responsibilities.

That if they make a mistake, if they see a mistake made, or they even believe or suspect that something is not right or even if they have a question, right,

about whether, what a specific rule is they are asked and obligated to raise their hand to report that. There's a number channels internally.

And no act of reprisal or retribution can be taken for the simple act of reporting, right. That is part and parcel of our culture. So I realize I talked a lot, put out a lot of information there. But I think there's some just contextual points in a very highly charged discussion that we think we need to get out there so that folks can start having a discussion around what's occurring, what's not occurring. And then obviously is it going to be a racy topic.

Judith Emmel: Thank you very much. We're going to move to the question part of our session today. Okay Operator, we'll take questions now if you can queue those up thanks.

Coordinator: Thank you. We will now begin the question and answer session. If you'd like to ask a question please press star 1 and record your name clearly. Our first question comes from Charlie Savage with New York Times.

Charlie Savage: Hello, can you hear me?

John DeLong: Yes

Charlie Savage: There was a reference in The Post article today to something drawn from a document that was not posted that referred to a weak selector search involving Ericsson Radar using the dish fire system. I'm not familiar with that system. Is that a 12333 system happening abroad or a FISA system happening domestically?

John DeLong: Okay, great, thanks for the question. I got that same question this morning, in a different context. So what was at the core of that was a query again as I talked about, a person making a query, right, that didn't comport with our minimization procedures. They didn't do it willfully, they did it, they essentially thought about combining a number of terms, right. That incident was detected, corrected and reported, right.

You asked about a specific system and a specific authority, I don't want to go too much into the details of systems and authorities. I think that we're conflating systems and authorities. I do think that you do bring up a very important point which is that there's a twelve triple three authority that NSA operates under regulated by executive order.

There are then a class of activities, right, that fall under the Foreign Intelligence Surveillance Act, right, and that involve court approval. Those are different authorities and I think the important thing that again, back to my prior comments is, there are different reporting mechanisms for each of those.

And so I want to make sure people understand that FISA incidents go through a number of mechanisms, vehicles, documents. Twelve triple three incidents also go through a number of mechanisms, vehicles and documents. And sometimes they're the same documents, like the one that's in the article. Sometimes they are different.

Judith Emmel: Next question please.

Coordinator: Next question comes from Mark Hosenball with Reuters.

Mark Hosenball: Reuters, yeah. Can you hear me?

John DeLong: Yes

Mark Hosenball: Okay, so I guess one of the questions that I'm, I want to ask is, I mean, if your compliance record and your compliance procedures are so rigorous and outstanding, why have you been so secretive about giving a public account of these mistakes?

I mean, Senator Wyden and at least a handful of others have been hinting for years about these, this record of mistakes and but they've been, in fact at one point, I believe the Senate Intelligence Committee, they proposed an amendment requiring you to report the number of mistakes or, the number in incidental collection incidents involving Americans and that was voted down in the administration and presume the NSA vigorously opposed that.

So why the secrecy about this if you believe your performance has been so good? And might you have not avoided some of the current uproar had you been more candid in the first place?

John DeLong: Great. So I think, you know, we, the point that everyone needs to understand is we don't hide these incidents, we don't keep them within NSA. They're provided through to multiple overseers through multiple channels across the court of Congress and the Executive branch through a number of heavily regulated pathways and mechanisms.

So I take very much to heart your point that now that we're having this discussion, right, going back, would it be appropriate, can it be appropriate, how can it be appropriate, right, to have more public information about NSA and activities. I think that's a very fair question.

Looking back historically, right, I think it's important that, you know, from a NSA perspective, and I think there's a, there's obviously a broader discussion to occur here, from a NSA perspective, we were striving to be as transparent as we could with our overseers across all three branches of government.

And I think that that's, right, you know, we're, I think, you know, I've been in discussions with multiple folks, we're looking at more ways to be more transparent.

Back about in about June of 2012, I started doing some interviews about compliance at NSA. Again, focusing not so much on just raw incident counts which can be I think both confusing but also not the only way to measure a compliance program. But we try to start to get out there other ways that we measure and talk about compliance the number of people we have, the resources we bear, the best practices we draw from industry.

I am speaking at a national conference on compliance in October, so there's a lot of different ways that we've been trying to get the message out. It hasn't always been, "Let us tell you the five mistakes we made on Tuesday and the seven mistakes we made on Wednesday," right, we do that with our overseers, we do that for ourselves. But I think your question is very much on point.

Coordinator: Next question comes from Toby Zakaria with Reuters.

Toby Zakaria: Hi, can you hear me? Hello?

John DeLong: Hello, sorry. Yes, I can hear you.

Toby Zakaria: Okay thanks. I'm wondering whether there has been any determination made yet about how Ed Snowden got the material out of NSA and whether you've

come across any actual hard evidence about whether the Russians and Chinese have actually accessed this information.

John DeLong: Thank you for your question. I am the Director of Privacy Compliance, I'm not the Director of Investigations. So I don't...

Toby Zakaria: But you hear stuff, I'm sure, right?

John DeLong: As do you I'm sure. So yeah, I get your question, I think we'll have to take that and, you know, go to DOJ or I'm just, may be DOJ may be not the right one. But...

((Crosstalk))

Toby Zakaria: Okay, can I ask another question? If you're not going to answer that one. This one. Has anybody been disciplined involving these mistakes and has anybody been disciplined over the Snowden leak?

John DeLong: So I'll confine my remarks to the mistakes. And I believe you're referring to the mistakes that are in the report that...

Toby Zakaria: Right.

John DeLong: As was in the article. So like I said before, everyone has a different definition of discipline.

If an analyst makes an error, right, and an analyst, I mean, we go back and then there's a, you know, a mistake again, we may in fact and have in fact, right, removed database access, right. I can't speak to every single one of these incidents, we haven't - I haven't had the time to go through methodically on each and every one of them.

I just want to make sure people understand that we take each of them seriously, right, these are unintentional mistakes, these are not intentional. We have a zero tolerance policy for intentional mistakes, right. But I really want, right, people to understand, and to understand that.

Coordinator: Next question comes from JJ Green with WTOP Radio.

JJ Green: Hi Mr. DeLong, and everyone, thanks for doing this and thanks for taking my question.

John DeLong: Absolutely.

JJ Green: In The Post, it's written, "In one instance, the NSA decided that it need not report the unintended surveillance of Americans."

And so my question from that predicates - is predicated by something that the other gentleman said a few minutes ago, saying that he wouldn't call this a cover-up, he would call it obfuscation. And wondering why would you not report unintended surveillance if it was an accidental mistake? And your response to that allegation that you've been obfuscating.

John DeLong: I would take pause with the term “obfuscating” but obviously everyone has a different definition of a word. So, you know, there's multiple things in the article that talk - there's one part that's very confusing, I believe which is a confusing of incident reporting with guidance that went out to analysts, right, on how to help our overseers actually do their job.

So there's one part of the article that talks about targeting access rationales and summaries of justifications for targeting. In those cases what we actually worked with our overseers, was a way to give a one sentence summary of the justification for a certain targeting. There is no intent to hide anything.

What's also provided to the Department of Justice and ODNI on each and every one of those is the gory details of why we believe a person is overseas and not a US person. So people need to understand that.

You know, back to your question of, you know, on any particular incident, right, is a decision not to report that particular incident was actually in a report that was actually sent internally, right? There's a number of different pathways that incidents go, right, you know, there's pathways that go to our internal overseers, there's pathways that go to our external overseers. So I just, I don’t want to give everyone the impression that obfuscating is what's going on here.

((Crosstalk))

John DeLong: I think part of the confusion, sorry if I may, is that there are multiple different paths and different thresholds for what constitutes an incident, right, what constitutes a reportable incident outside, right. We were, just to maybe add more context here, we have internal policies that go above and beyond the procedures. We actually internally report those as incidents.

Because they're violations of our own policies and reason we do that is because a stitch in time saves nine, right. If we can detect something where there's confusion or there's a mistake and we can correct it there, we can do so before we cross over the line of law, policy or regulation.

JJ Green: So you explained all this - and this is just a quick follow up - to him, I'm asking, did you explain all of this to him? And why is there no evidence of this in the piece? Did you explain all of this to him?

John DeLong: So, I don't want to dissect to much the particular story. I think, it's in the story. We spent 90 minutes of conversation; a lot of what I raised in the beginning was more or less the same. Maybe not word for word but the concepts - ideas were there. I think part of this, is it's a difficult subject, right, and it's all coming out very fast, so that's it.

Coordinator: Next question comes from Ken Dilanian with the LA Times.

Ken Dilanian: Hi Mr. DeLong, thanks a lot for doing the call. Two questions. One, to the extent that US content, US person content is inadvertently collected, what happens to it? Is it always destroyed or are there some cases when it can be stored?

And then secondly, can you talk about what the error rate might be on the phone database program, you know the metadata program? Because there's some analysis out there that suggests, based on this report, that it's pretty high, like between 8% and 30% based on the number of errors related to the MARINA database.

John DeLong: Okay, I think two questions there. So one was - and I mentioned this before, if NSA does inadvertently collect, you know, communication from or to US person, while, for example, collecting against a non US person overseas.

Let's just take that hypothetically, you asked, "How can the NSA use that information? What can they do with it?" NSA operates under nearly a dozen different regulatory regimes different minimization procedures.

And so, what you really have to do is look to the, look to the actual rules within each of those minimization procedures that contemplate how and what we can do, right. That I think is just, that's just a part of the reality of how NSA operates, right. It's very important for people to understand that.

There's not one person at NSA, one database, one authority, right, and one collection point, right. Our activities are regulated through multiple different means, right, through multiple different authorities, right. You know, and you can count them different ways, I generally count them about a dozen, that's just sort of how I think about it in my head, as a director of compliance. And analysts and systems have to work across those, not all of them, some of the things.

And that gets me to, I think, your second question, which was on the call metadata program, right, you asked about error rates. So, you know, that is actually an activity that we have special emphasis on and we have since, you know, since 2009 and before.

We recognize the sensitivity of that program, right, and we have in place a number of technical safeguards, right. And a number or procedural safeguards, a number of training safeguards. A lot of overlapping safeguards in that.

You know, again, I think back to the prior question about, you know, are we going to report numbers of incidents in that, going out? I think that's something we're looking into. That's something that we have reported to our overseers. I actually think our track record on that has been very solid from a compliance perspective. I wouldn't, I think your numbers you used of 30% those don't resonate. Those are not right.

Ken Dilanian: Okay.

Coordinator: Next question comes from Saundra Torry with USA Today.

Saundra Torry: Hello, thank you for doing this. In the Gellman article today, it mentions a serious incident in which a court order was violated with unauthorized use of data about more than 3000 Americans and green card holders. Can you tell us what that error was? And what precisely to whom that was reported? Congress, the FISA Court or who. Or was is not reported?

John DeLong: Great, I can do that. You're all thanking me for doing this. I feel like, you know, I should get - no, I really thank you, this is really a good opportunity to get context out there and to really get some of our things.

So I believe the, sorry, not believe, I know, that what you're talking about is in that 13 page document, there was one incident related to the head of our FISA unit.

And that particular incident, what NSA found was in archived backup media. It's not accessible to analysts, only accessible to trained personnel, right, a number of records that had gone beyond the retention period. So everything that we have, has a set retention period, number of years, etc.

You know, there were not 3000 persons over 3000, right, filed records there. There were no analysts was looking at those, right. Those were there as we were doing a routine review. We discovered these, they were beyond the retention period. We immediately deleted them. We reported it both internally, we reported it to the Foreign Intelligence Surveillance Court and we reported it to Congress.

So, I think that, you know, it's getting confused in the discussion and thank you very much for the opportunity to correct the record.

Saundra Torrey: Can I ask one other question?

John DeLong: I don't play that ground rule, so whatever Vanee says. The director...

((Crosstalk))

Saundra Torrey: The broad question is the head of the FISA court basically says that they lack the tools to independently verify the information you bring to them. So their oversight role doesn't really sound like much oversight. Yet NSA officials have been citing that as one of the major ways that we, the Americans should be sure that these programs stay within the law.

If they don't have anything to verify these questions by, how can that be an important oversight?

John DeLong: Great. I think I'd make three points. I think, a little bit, there's a confusion between just how documents flow in and out and how the court functions. And I thought the court statements were very thoughtful on this. Because we recognize that the accuracy of the documentation we file in front of the Foreign Intelligence Surveillance Court is paramount. And we recognize that.

We also report to the court incidents. And I can tell you they take every single one of them seriously. They ask multiple questions at times, follow up, right. They want to know what's going on. So this idea that it's just a flow of documents that go in and a flow of documents that come out has got to be put to bed. So again, let's not confuse flow of documents and - with incidents, etcetera.

So the other thing that's important to know is it's not just the court. There's the Department of Justice, also Director of National Intelligence, DOD, all of whom play a role in oversight of activities, right, that occur under Foreign Intelligence Surveillance Act. So - and the important thing too is that these are not just, again, sit back and review reports.

These are active, on site investigations, reviews of activities. In fact the thing I mentioned for a previous call about the summary, so that our overseers would get a quick idea of the rationale for a specific collection request. They review each and every one of those. They're here, they are at NSA, right. We don't, we - they come here, we show them exactly what the records are. They come and review our activities.

We've even had the Foreign Intelligence Surveillance Court up here. These are - there's a lot of active engagements. This is not just papers flowing back and forth.

At the end of the day it can look like that, but there's a lot of people involved in this process that care a whole lot about making sure that NSA follows the rules, making sure our overseers carry out their statutory and other requirements. And making sure that the people who authorize our activities

are confident in our statements, right, and have a mechanism to, right, make sure that when incidents do occur, they understand.

So, there's a human element to this story that has not come out yet. And it should, which, there is a whole lot of dedicated people here at NSA, there's a whole lot of dedicated people in the oversight compliance context, there's a whole lot of dedicated people out there that are really trying to get this right. And I will leave it at that.

Coordinator: Next question comes from Adam Levine with CNN.

Adam Levine: Hi, thanks for doing this. Two questions for you. The first is about the, just the numbers of violations. And, well you've said the bulk are technical or unintentional. I'm just wondering, are there any that were intentional oversteps or violations? And what were those if you could describe them in any way?

And the second questions goes to just Congress and given - the article sites the low number of people that have the security clearance to get briefings on this. And I'd just like to get your take on congressional oversight and your ability to deal with Congress if so little percentage of those that brief there congressional members are actually able to be briefed on these programs?

John DeLong: Yeah, Great, thanks for the question. I may just ask you to just repeat the second part, but I'll try to get the first part. I think what you were asking was, we talked a lot about unintentional and mistakes and just the natural the idea that people are human and they do in fact make mistakes and NSA is dedicated to correcting and detecting and correcting those, right. None of them are - no one thinks a mistake is okay, right.

Any willful violation of the rules is taken very seriously and reported to our Office of the General Counsel, and the Inspector General. And appropriate personnel action will be taken, right. And I think I need to leave it at that.

Again, I've been Director of Compliance for four years and I can tell you that folks are dedicated to following the rules because they know that their activities are being recorded and reviewed. And they know and they come in and they self-report. And that I think is critical. May I ask you for your second question again? Sorry.

Adam Levine: Just to clarify, are you saying there have been, sort of, willful violations. It's not just technical or unintentional violations.

John DeLong: Yes, so yes, there are rare violations of a - those are taken very seriously, right, and those are reported. You know, I think the other thing is, you know, it's not always necessarily just in the conduct of surveillance. So, there may be other reasons why they are - have been removed. And so I just want to make sure that's clear.

But I realize there's been a lot of statements about violations and abuse. And those are all, you know, people need to understand, right, NSA is very dedicated to the law, right, we are very dedicated to following this. When we make mistakes, we detect, we correct and we report.

Coordinator: Next question comes from Chris Good with ABC News.

Chris Good: Yeah, I guess just following up on that last question. Can you tell us how many of those rare incidents have - incidents have happened? And then the other part of my question is, we're sort of focusing on this report and if I am

reading it right the date on this is May 2012. Is there anything, either willful abuse or just a significant accidental brief, that's happened outside the time frame of this internal audit that you can tell us about?

John DeLong: So, you know, I don't have the numbers here. They are extremely rare. You know, I can't - when they do occur, right, they are detected, corrected, reported to the Inspector General and appropriate action is taken. I really don't have the numbers here with me, right. What I can tell you is they're extremely rare.

The process that we run inside NSA for oversight and compliance is one where, right, there's a whole process for detecting and correcting incidents. The number of willful violations is miniscule, I mean tiny. And I'm not talking like the percentages we're talking about I'm talking, you know, I don't have the exact numbers, but a couple over the past decades. Right, we're not talking about anything. Sorry, can you repeat your second question?

Chris Good: Yeah, is there anything outside the timeframe of this audit that involved a significant number of people's information. Briefs, either accidentally or willfully that you can, that you can tell us about?

John DeLong: Sorry, I don't entirely, you're talking about the scope of a single, the quarter that was, that you're looking at? Is that what you're talking about?

Chris Good: Yeah, we're focusing all these questions sort of what's on The Post story and...

John DeLong: Right, yes

Chris Good: The Post story focuses on a specific audit. I'm wondering if there's anything major that's happened after the timeframe of that audit?

John DeLong: So I - it's a continuous process, I think that, and I know that the administration and we are looking at ways we can be more transparent in numbers and context, right? To go out to, right, to go out to, right. Yeah, so I think we're looking at ways, I think it's important to note not just what NSA's saying but, right, what has been in the Senate report. That's there's been no willful violations of the 702 authority, right?

There's other statements out there and, you know, someone who's, I guess you could say been on the inside, right, and I've seen that and that Senate report is spot on. So, you know, it's not just us, but its folks that are also receiving the incident reports are overseers, right, and understanding what's occurring. Folks need to understand that.

Chris Good: Thanks.

Coordinator: Next question come from Siobhan Gorman with Wall Street Journal.

Siobhan Gorman: Hi, thanks again for doing this. One of the other things that is discussed briefly in The Post story is the October 2011 incident where the Foreign Intelligence Surveillance Court ruled that the collection effort - this collection effort was unconstitutional. I was wondering whether you could provide for us a little bit better sense of what the scope of that activity was? And what was done to rectify it?

John DeLong: Sure, thank you all for thanking me again too, I feel like I should thank you. It's just -a so the issue you're talking about, if I'm following is that the 2011 issue that's been mentioned where the court found at least in part our procedures were, there were constitutional and statutory issues with our

procedures. So, that incident was discovered in 2011, right. We immediately reported it to the court and to Congress, right.

We then worked - we then worked with the court and in fact Congress to understand right? Number one, understand the issue, make sure everyone had a common shared understanding of what was occurring, right.

It was essentially a complex sort of technical issue about the interaction of our systems with, right, the communications environment. You know, again, no willful intent to, right, to do anything more than try to get things accurate and precise in documentation, right.

We then worked with the court, we then developed, right, we kind of got ourselves more in line, right, and we made sure that then - and we got to the point, actually, where the court reauthorized the activity, under different procedures to account for that technical way that our systems interacted with the communications environment. Right, I'll leave it there.

Siobhan Gorman: But can you say anything about what the scope was of the violation or the concern on the part of the court that you later rectified?

John DeLong: So, the - internally here we're working through, I believe, a - not believe, I know, a more fulsome answer to that but we believe it’s important for certain additional documents to be added to the discussion. And our concern is too many more sound bites in this issue will further confuse what's already - and I hear you exactly Siobhan, it's confusing to hear it in little bites and sound bites.

I think there's a, there's a set of documents and a set of broader things that need to be brought - and, you know, I wish I could hand them to you today over the phone, that would be quite amazing...

Siobhan Gorman: Me too.

John DeLong: ...but, right, we're just not there yet. So.

Siobhan Gorman: Okay.

Coordinator: Next question comes from Dan DeLuce with AFP.

Dan De Luce: Yes, if you could just clarify and elaborate on one particular incident mentioned in February 2012 that supposedly involved the retention, the unlawful retention of more than 3000 files that FISA court has ordered the NSA to destroy. Could you also, kind of, go over that whole episode?

Vanee Vines: Dan,Vanee, so that was discussed earlier, so we'll just give you the quick summary.

John DeLong: Sure, is that okay? So there was a similar question before. I'll, you can queue in when I get the right -- so that incident is in the document that was in the article, right that involved a retention - this involved archives for the backup files, right. Not accessible to analysts; accessible to trained personnel that understand the authority under which that information was collected, right?

So what, there were 3000 records, if you will in those files, right, that were kind of in a backup archive, as they were going through and further deleting what they found, discovered was that there were those 3000 records that had been retained longer than our procedures allow them to be retained.

So what do we do? We reported it, we deleted the files, we reported it both internally, we reported it to the Foreign Intelligence Surveillance Court, we reported it to Congress. So, I think that's more or less, kind of, the major points we hit before.

Dan De Luce: And then do you have, do you use, you said earlier, that you wanted, that you're looking at other ways or more ways you can be more transparent. Doesn't this, since your acknowledging that these documents that are in the newspaper report are accurate, and as you say, these incidents, in your view, are not willful misconduct.

Isn't this a case where secrecy has just - is your worst enemy right now. Wouldn't being more transparent about these incidents give the agency more credibility not less?

John DeLong: I think those are all points we're taking under consideration. We're working on the release of more documents soon, right. Again, I think, and I, if I'm understanding the tone and the sort of background of your conversation is that people do need to understand that these are not willful violations of right, there's no willful violation here.

These are mistakes, right, and the fact that that document even exists, sort of, I think the story that hasn't come out is the fact that that document exists is actually evidence that we take each and every mistake very seriously, right, that, you know, you know, these mistakes look, you know, in the context, they're in the parts per million, parts per billion range.

So we understand that when you look at them in just a raw number, right, they can, right, they reflect, you know, part of the fact that we really do look for them, right, detect them, and then correct them.

So I think you hit it right on the head, which is transparency, right, you know, without being translucent, that's my usual comment, transparency is absolutely critical to this. Again it's not just our, you know, it's not just our view, it's what we've reported to our overseers, right, we want to make sure that people really understand this.

Sorry, one more, right - people need to understand, and I think transparency will help but these are not willful violations, they're not malicious, right. These are not people trying to break the law. These are people really working hard on national security, right, in an environment with data, with machines, with humans, with, right, lots of training behind them, right.

But we really need to make sure we have technical safeguards in that, we need to understand, people, these are not willful violations, right these are mistakes that are made that we detect, we correct, and no one at NSA from me to anyone else, right, thinks that any of these mistakes are okay. People need to understand that.

Dan De Luce: So just one follow up. Is, there's another impression though that is left by all of this which is, another factor which is the kind of incompetence or inadvertent concern that the agency simply can't possibly manage so much data flowing in at such an incredible scale.

John DeLong: So I think your question was, so, you know, kind of, the absolute versus percentage. We, our job is to manage data, right. That's part of what we do. And again, what, I think the confusion comes from, we generate a lot of

reports every time we make a mistake. If we generated the same number of reports every time we did something right, it would maybe go to the moon and back.

I don't know exactly what it is, but people need to understand that, right, that the squeaky wheel gets the attention. What people need to understand is that, we do, and again, you know, I talked about 20,000 queries, or 20 million, yeah 20 million queries per month, right? Those are correct, those are correct. Occasionally we make a mistake; we detect it and correct it.

Vanee Vines: We have time for one more question.

Coordinator: Marc Ambinder with The Week. Your line is open.

Marc Ambinder: Yes, I just wanted to, I noticed that many of the mistakes were caught by active - something that was referred to as active alerting and active auditing. Could you explain a little bit about what that process entails?

In other words, when an analyst is working with a (selector) queries database, particularly if it's a potentially involves FISA material, does that mean that everything the analyst does every keystroke is recorded, and there are internal audit systems that automatically monitor those queries for compliance as well as the post facto dipping into the target folders and sort of sampling to see what happens?

John DeLong: So I think that the general answer is yes. The more specifics that I can say is that we do watch what people do, we watch what machines do. I really thank you for pulling out that part of the report.

I don’t think it was, you know, a major factor in the discussion yet, which is, we do in fact have a lot of technical and process based things to rapidly detect for example a person that (rose) into the United States. There's a text for example, a query such that queries are recorded, right, provided to somebody else for review. They're subject to audit. Those kinds of things.

Those are built into our compliance regime. They're built into our oversight structure. And so that, you know, people have not focused too much on how we detected these, and you'll see if you look at the graph, you'll see other things like self-reporting, and that.

But the majority of the ways we detect these are by actually going out and looking for them. And that’s, you know, that's the sign of an oversight and compliance program that’s dedicated, that’s working and that a sign of, right, people that are not committing willful violations, but people that are really doing the right thing.

Vanee Vines: Ladies and Gentlemen, I'd like to thank you for joining us today. We'll have to conclude our session. For those of you that may have come in late, you’ve been talking with John DeLong, the NSA Director of Compliance. If you have any additional follow up you can please send an email to pao@nsa.gov.

Again we really appreciate the time to correct some misperceptions out there. It was very important to us. We hope our passion on the subject came through and thank you again.

Coordinator: This concludes today's conference. Please disconnect at this time.

END