BACKGROUND BRIEFING BY SENIOR ADMINISTRATION OFFICIALS ON FISA

James S. Brady Press Briefing Room - The White House

February 26, 2008 - 2:40 P.M.

SENIOR ADMINISTRATION OFFICIAL: I appreciate you taking the time to discuss this issue with you. I just want to give a very brief overview. I know this is a very complex subject and a lot of discussion out there, and it's hard sometimes to follow it.

Let me start. Foreign Intelligence Surveillance Act of 1978 passed because of the abuses of the 1960s, 1970s, and frankly, prior to even that time frame. There was a balance struck in the 1978 act for the intelligence community, and it said, if you're doing your foreign intelligence mission overseas, you do not need a court order to do that mission. It specifically exempted the international signals intelligence activities that our community does.

Q You mean it said you could break the law?

SENIOR ADMINISTRATION OFFICIAL: No. What the law said was that if you are doing your foreign intelligence mission, looking at communications abroad, you do not need a court order. That is what the law said. Okay? And --

Q -- by Congress?

SENIOR ADMINISTRATION OFFICIAL: Okay, that's what the Foreign Intelligence Surveillance Act of 1978 did, and that is what the legislative history specifically says, and that's what the Foreign Intelligence Surveillance Act says. I can get you the actual text. We can furnish that to you. I mean, it's plain as day. I could pull up the quote right now that says this law specifically exempts the international signals intelligence activities conducted by the National Security Agency.

What it said, though, is if you're doing your mission here in the United States you need a court order. So if you're targeting a U.S. person here in the United States, to intercept their communications you need to get a court order. That was the balance that was struck in 1978.

In 1978 -- let me divide the worlds of communications into wire and wireless -- 1978, wireless communication; radio and satellite, primarily for our international communications system. Fast-forward to today -- 90 percent I think, or so of the international communications systems carried in a glass pipe; a wire, for purposes of FISA. So we've had a huge shift from what was radio and satellite in 1978 now to wire, to fiber optics -- a huge, massive shift. The international communications system is also routed through the United States in many cases. Extraordinarily cheap to use this fiber optic system, a large price advantage over other types of wireless communication.

What caught us -- what got us caught up was, in 1978, when they did the law, when they thought

of wire, they thought of privacy, and if you're on the wire that is what they use to define when we would need to get a court order, exempting this international activity by exempting out the radio and satellite communications mission that we do.

So we had this shift. I think in this debate, I think everyone has agreed now that FISA needs to be modernized to reflect the technologies of today; that they wrote FISA in 1978 to reflect the way the technology was then. I think everyone is basically on board with the fact that we need to have FISA modernized.

That brings us to the Protect America Act and the passage of the Protect America Act. The Protect America Act said, if you are targeting a foreigner overseas, you do not need a court order. But it went one step further than what was even in the 1978 act. It said, for your targeting procedures, to intercept that foreign communication you need to have those procedures submitted to the FISA court and approved by the FISA court. In 1978, our mission to target international communications, the FISA court had no role in that.

We did submit those targeting procedures in August. The FISA court approved those in January of this year.

Obviously, lots of concerns about some of the language of the Protect America Act. For the past six months, we worked very closely with the Senate on their bill. That bill responds to a lot of concerns raised by the public and by members. It expands the role of the FISA court even more in the foreign targeting procedures. Not only does it say that these foreign procedures -- that the procedures that we're going to use to target foreign people overseas have to go to the FISA court, but now the documents signed by the Attorney General and DNI that authorized this acquisition activity have to go to the FISA court. And in addition, something called "minimization procedures" are now going to have to be approved by the FISA court. None of this was part of the balance struck in 1978.

Let me pause and talk one minute about this word "minimization" that you've heard. Somebody is going to ask me the question: But when you're targeting a foreigner, don't you get a U.S. person sometimes? And the answer is, yes. And the answer is, for many decades we have encountered information to, from, or about a U.S. person when we're doing our overseas foreign intelligence mission. The way we deal with that is a process called "minimization." That's a whole separate briefing that Dana probably does not want me to give, but what that basically means is that we minimize the information concerning the U.S. person. And there's elaborate procedures that are a part of that.

That is not anything new. Minimization procedures are mentioned in the FISA - - in the act of 1978. It's something that was recognized would be a part of our intelligence community process.

So we are trying to basically restore the balance that was struck in 1978 through this legislation. That is the goal. In fact, what we've restored -- yes, we've restored the balance, but we have a greatly enhanced role for the FISA court, compared to anything that was done in 1978. And certainly the Senate bill expands on that role, in addition to a whole set of oversight procedures and reporting requirements that are in that.

This brings us to immunity and the issue of immunity. The bills have prospective liability protections, so going forward with our activities. Then there's the issue of what to do about retroactive liability protection. And this involves the program that the President spoke about on December 17, 2005, in his radio address.

The Senate committee report is perhaps the best source of information about this. I would commend all of you to read it. They did an exhaustive analysis of this. The bill passed out of the Senate Intelligence Committee 13 to 2. Of course, you know it passed the Senate with 68 votes.

What do they say in that report? They say it's absolutely vital to our intelligence community mission that we have the cooperation of the private sector. It says that their help is indispensable to the safety of the nation. It also says -- it goes through what they call the unique historical circumstances after the attacks of September 11th, the fact that the private parties were given documentation showing that the President had authorized the program, and showing that the legality of the program was also certified by high-level administration officials. It said that they had a good-faith basis for cooperating with the government. It does not make a judgment about the ongoing discussions about the respective powers of the Congress and the President, and make an ultimate legal determination about that program.

What is it from the perspective of the private parties? What are those who are alleged to have assisted with this caught up in, and what is the problem? Well, first, they can't defend themselves. And you say, well, that's our fault because we have asserted state secrets in various lawsuits. And the answer is, we have. And the reason we've done that is because the only way to defend yourself is to go out and describe the exact activities that I am talking about, and that would be a very bad idea if we want to continue to gain vital information, particularly in the counterterrorism arena. Second, they did act in good faith, in reliance on the documents that they received and are discussed in the Senate committee report.

With that, I guess I would just leave you with -- kind of in summary, if I had to reduce this and try to make it simple about what we're trying to do, three basic principles that the Director has always acted on: One, no court order to do our foreign intelligence mission. Let us do our foreign intelligence mission targeting foreigners overseas without a court order. That was fine in the Cold War of 1978; today we face, frankly, a more dynamic enemy than we faced in 1978 in terms of their ability to exploit our technology and to change their procedures, compared to the Soviet Union that we faced.

Second, a court order for targeting Americans. Something that is overlooked in the Senate bill, for the first time a court order is required if we are targeting an American anyplace in the world. That was not deemed appropriate in 1978; now the Senate has deemed it to be appropriate. That would be a large change. Prior to -- frankly, the way it is today, we go to the Attorney General to authorize those activities abroad targeting an American. The Senate bill would change that.

And finally, we need to have liability protection for the private sector, both prospective and retroactive, and we need the ability to compel their cooperation.

With that, I'll have [my colleague] --

Q If I could ask you one question on something you said?

SENIOR ADMINISTRATION OFFICIAL: Sure.

Q What are these targeting procedures that were approved in January? And if the court has already approved these procedures, then why do you need the -- do you need the law?

SENIOR ADMINISTRATION OFFICIAL: Well, the law has expired, so the court has approved procedures that are part of now, frankly, an expired law. So first, what are the procedures? The procedures are, how do we determine if somebody is reasonably believed to be outside the United States? How do I know that when I am going after somebody to get intelligence information, how do I know -- right? We want to make sure that they're overseas and that they're not here in this country. So that would be a concern, do we have adequate procedures that we're making sure. Now, there's a lot of technical ways to do that and other things that we've laid out for the court, and that's what they've approved.

Q And these are now no longer -- the approval is no longer valid because the law has expired?

SENIOR ADMINISTRATION OFFICIAL: Yes. The law, of course, has expired --

Q So does that make the approval, the court approval of these procedures invalid?

SENIOR ADMINISTRATION OFFICIAL: Well, we're still operating under those procedures. There is some activity that continues past the expiration of the act. And there's some --

Q Until August?

SENIOR ADMINISTRATION OFFICIAL: There is some activity that will continue past the expiration of the act. We have said that we issued some -- what are called "authorizations for activities" in August. So those authorizations would last until this coming August.

But, lots of confusion out there. These authorizations are authorizations signed by the Attorney General and DNI that authorize the activity. So it says, yes, agency -- pick your agency -- you are hereby authorized by the Attorney General and the Director of National Intelligence to undertake the following activities; and here are the rules and procedures you're going to follow, and you're going to file the procedures with the FISA court, and here's how you're going to act.

Separately -- so that just gives us the ability internally to go and do this activity. Separately we have to issue directives to private parties to cooperate with us. We can't do those activities under the authorization without the help of the private parties.

So now that the law is expired, that has led to great concern on the part of our private parties. It's also in great question whether or not we could issue new directives to new private parties. So, yes, the authorizations, which are enabling documents that give the authority to our agencies to

act, continue past the expiration of the act. But if I need to issue new directives to new private parties, or to modify the authorizations and directives that are already out there, I have an expired act, and that is something that would lead to great concern.

Everyone assumed that under the old authorizations we could continue the activity we were doing, and add, essentially, new information to those same activities. We found in the last week that even that piece of information that we thought everyone was agreed on, and we think our arguments were strongest on, we had problems with that in the last week.

Q So, basically, you cannot conduct -- get this activity without help from the private telecommunications firms?

SENIOR ADMINISTRATION OFFICIAL: "Electronic communication service providers" is the way I would phrase it, but, yes, private parties --

Q Right. And so because the law has expired, they're the ones, because they do not have the immunity --

SENIOR ADMINISTRATION OFFICIAL: They have lots of concerns. They've seen that companies have been sued. They have to protect their shareholders, they have fiduciary duties, they have all of those responsibilities. So we can make very strong arguments that these things continue even past the expiration of the act, and you've seen discussions of that in the public sphere. We can make those strong arguments, but they're the ones --

Q If they're acting legally why do they need the immunity?

SENIOR ADMINISTRATION OFFICIAL: Ma'am, your question about targeting procedures, I think that's a good question, because it goes to sort of the internal logic within the Protect America Act. What's lost in this debate is that there is sort of a good, common-sense basis to the Protect America Act and the legislation that we want to see made permanent. And it is basically what [my colleague] described, that FISA if you take -- if you look at the scope of potential surveillances out there, FISA in 1978 was intended to cover this scope, this part of it, which was targeting surveillance within the United States. Because of the change in technology, it started to creep out and cover the whole field. So Congress -- and I think there is a consensus on this -- said, wow, we need to bring it back to what we originally intended; we shouldn't be giving Fourth Amendment protections to terrorist suspects overseas.

How do we do that? We create a scheme that says, you do have to go to the court and get approval, just like you always have, if you want to target someone living in the United States -- under traditional FISA. But if you, the government, the executive branch, want to target somebody outside the United States, you just have to have procedures that are -- that reasonably determine that the person you want to target is outside the U.S. If you have procedures in place that say, "Check this, check this, check this," and the conclusion is that person -- we expect that person is outside the United States, and those are reasonable procedures that reasonably lead to the conclusion that the person is outside the U.S., based on that conclusion we should be able to go ahead and target that person for surveillance without having to go to FISA court.

And so in the debate, that is a very common-sense notion that gets lost, I think, in the debate. We had a really good, sound process in place in the Protect America Act, and that is, of course, incorporated pretty much into the Senate bill. And that's what we really need. We need that flexibility to be able to go up and do that surveillance overseas without having to go to a court, show the Fourth Amendment probable cause standard -- what was designed for people within the United States -- when they're trying to target someone who's maybe in a cave over in Afghanistan.

Q But that's not what you're arguing about in Congress. No one in Congress has disputed the notion that you should have the ability to target foreign-to- foreign communications. I mean, the most liberal senators, Russ Feingold and Senator Dodd have acknowledged that months ago. So why not argue about what's left to argue, which is the immunity question, and leave this behind? This seems like a bit of a red herring, to be honest.

SENIOR ADMINISTRATION OFFICIAL: Well, no, I said that there's consensus on this. And I think people tend to forget that this was a very well-thought- out process. I mean, we've been involved -- we spent half our life up on Capitol Hill over the last year in briefings and hearings. And I'll tell you, the experience, at least from my perspective, is that it was a -- it's been a very healthy legislative process. I mean, every aspect of that scheme that I just laid out and the immunity issue has been hammered on from both sides and debated. And the result was a very solid, well-thought-out bill out of the Senate.

And the bill, of course, incorporates not only that scheme I'm talking about, not only immunity, but also, as [my colleague] said, a lot of limitations and protections that weren't in the original Protect America Act.

So one of the reasons why I think you're seeing sort of a strong effort on the part of the proponents of the Senate bill is because we saw the legislative effort that went into that product, and we know that it's very sound. And you're not going to find any piece of that legislation that wasn't really carefully debated on both sides. And we think that with a bipartisan majority that passed it, it should be taken up in the House.

SENIOR ADMINISTRATION OFFICIAL: So let me address the question, then, of -- we were asked to kind of give an overview of the whole issue, so you had kind of that broad context about our mission and what we're trying to do in the legislation and how critical the private sector is to this. Certainly the past week has reminded us very clearly that no matter how strong our statutes and arguments, we really do need the willing cooperation of the private sector, who have different issues and other issues to consider besides just the national security.

There is a debate over the activities the President authorized after 2001. The Senate committee report acknowledges that debate and says they are continuing to review that matter. There's heated disagreement about that matter. No doubt about it. And the issue, though, is whether in this heated disagreement between the President and some members of Congress about the scope of people's powers under the Constitution -- the scope of the President's national security powers, the ability of Congress to pass certain statutes -- whether private parties are going to be the way

to play that out, and essentially, while our intelligence capabilities continue to degrade, is that how we're going to settle those issues, many of which have gone on for over 200 years? Why should private parties be caught in the middle of what is ultimately a debate over separation of powers and between the branches, no doubt a debate that people feel very strongly about, but these are private parties who acted in good faith to help protect the nation.

Q But did they act under law? They knew they were acting under the law?

SENIOR ADMINISTRATION OFFICIAL: Yes, the Attorney General --

Q Why give them immunity if they were legal?

SENIOR ADMINISTRATION OFFICIAL: Because to show that somebody was acting under the law, under the allegations and the numerous lawsuits that were filed, first they would have to show what exactly was done, they would have to show whether or not they engaged in the activity --

Q All they have to do is get from the White House -- say we gave them permission under the law.

SENIOR ADMINISTRATION OFFICIAL: Well, if the Senate committee reports suffice, which says that the President authorized this, and the legality was -- assurances of legality were provided to them, I wish that were sufficient to make the lawsuits go away. But that's not sufficient.

Q -- go along with that they were legal when you say they're legal, when the government says they are legal, acting under the law?

SENIOR ADMINISTRATION OFFICIAL: Well, we've seen there are, what, 40- some suits out there right now, and we've seen --

Q So they think they must have something. They think they're valid, don't they? Their lawyers obviously do.

SENIOR ADMINISTRATION OFFICIAL: Well, I'm not going to speak to what the lawyers of the other parties think. But bottom line is that some of these cases have gotten some traction. But we have been resisting on a number of different grounds. The problem is, is that aside what effort it puts us to, the providers are being sued. And they are in a position where they can't really defend themselves, because this is all classified, confidential information. Their reputations are in some danger, they go through the expense and the disruption of a litigation process, all because they really stepped forward and were good citizens after 9/11. And it's just --

Q Well, you can't just show the judge the classified information and let them make a decision?

SENIOR ADMINISTRATION OFFICIAL: Well, what we've done is we've shown this to members of Congress, and to the Judiciary Committees and the Intelligence Committees, shown

the documents -- the documents that contain the assurances that were given from the administration to the providers at the time when they were asked to assist. And those -- the Senate intelligence report, as [my colleague] said, found those were good faith -- those were assurances that the program was legal and that it was directed by the President, and that the providers had a good-faith basis for going ahead and stepping up and assisting the government and protecting the country against another attack.

Q I just have one more question. I know I'm being -- don't mean to monopolize -- but can you honestly say that no American has been wiretapped without a warrant in this country -- has not been wiretapped -- has been wiretapped, yes, who has been wiretapped without a warrant -- warrantless wiretapping in this country.

SENIOR ADMINISTRATION OFFICIAL: The reason I hesitate is because, as [my colleague] said, we will target surveillance against somebody overseas, and that person might -- 90 percent of the time that person is probably talking to people overseas, but sometimes that person is talking to somebody in the United States, and we intercept that communication. And as we've always done, we review that communication, and if it's irrelevant, we minimize it.

Q What do you mean, minimize?

SENIOR ADMINISTRATION OFFICIAL: Well, this is what [my colleague] was talking about. If it's an American -- United States person -- let's say we're targeting somebody, a terrorist suspect in the Middle East. That person calls over to an American phone number and gets a United States person. There are minimization rules in place that the intelligence community has been following for decades, for whenever they do target surveillance overseas they follow these rules. And if that communication is captured -- and [I], United States person, am on that phone call, there are rules that limit the dissemination of information about [me,] because I'm a U.S. person. My name can't be disseminated in intelligence reports in this kind of thing.

So there are protections in place to protect the privacy of Americans, but still allow us to target surveillance against targets overseas, where we really need to find out about threats.

Q Without a warrant?

SENIOR ADMINISTRATION OFFICIAL: Without a warrant, yes.

Q Just a couple things -- just so I make sure I understand. It would be the administration's position that these companies acted in good faith after 9/11, had the order from the President and, therefore, should be shielded from liability -- but you're seeking immunity retroactively in case the courts see it differently.

SENIOR ADMINISTRATION OFFICIAL: Yes. I mean, the -- I wish -- I certainly wish the process were that we show them the Senate Intelligence Committee report, file a classified declaration and the suits are dismissed and go away. That is not the way our system works. There's possibilities of discovery; there's appeals. We could get you lots of information about the different suits, the appeals that have happened, those types of things. Each one of those cases

runs a -- I mean, from our perspective, runs a risk of disclosing our sources and methods, each kind of a little bit more as more information is out there.

So from the intelligence community perspective, that is of great concern. And while we wish it were that the Senate Intelligence Committee report or our classified declarations suffice to simply dismiss all the lawsuits -- I'll defer to [my colleague] on litigation matters -- but that's not exactly the way it works.

Q I think I understand that. So I guess my next point is, I mean, I've seen it happen in a lot of cases, like, when you have national security, where the government intervenes and asserts state secrets, and gets -- I mean, I've seen cases that, plaintiff, you may have the greatest case ever, you're out of court because the government successfully asserts state secrets.

So I guess my question is, isn't that another approach? Can't you go in there and try to win on state secrets, and get these cases -- and, therefore, you've done something on behalf of these telecoms who you say patriotically helped? I mean, there are other ways besides retroactive immunity.

SENIOR ADMINISTRATION OFFICIAL: And that's -- those are the ways we've been pursuing so far. But as [my colleague] said, that sort of puts the -- the providers are still in an awkward position because they've got these complaints, these claims against them, but they're precluded from actually litigating them and defending against them. So it's actually -- that's not ideal for the providers, and it's not ideal for us, because we can't predict exactly how every one of these litigations is going to go.

And if I could add on to this, [my colleague] enumerated a couple of the reasons why it's important that the providers get immunity. One is just because -- these people stepped up to help and they did so as good American companies, so we shouldn't subject them with litigation. Two, as he said, the fact that in these litigations, we really run a risk of disclosing classified and very sensitive information about our most sensitive intelligence programs.

But don't underestimate the third thing, which is we have an interest in this, which is we really do -- as somebody said over here -- we rely on the providers to cooperate. We don't own the communication systems. We have to work with them. And, yes, we can compel them to assist us through various court orders or directives. But I know as a prosecutor working criminal cases, trying to get telephone records, there's some companies that work well with you and you get them in a day, and you can -- that will help you to run down the bad guy more quickly. Others will take the full two weeks. And so there's cooperation, and there's cooperation.

Also, keep in mind that, yes, the providers, if they want to, they can litigate everything we give them. They have the right under the PAA -- the Protect America Act -- to go ahead and challenge these directives, and that's within their right to do so. And at the end of the day, we might prevail -- we will prevail because we have the authority to do it. But during the time that that's being litigated, the surveillance we're asking them to do is not happening. So there's some foreign intelligence target out there we think we need to be able to surveill, we're not surveilling that person. So we don't know what information we're missing.

So don't underestimate -- because there's no immunity, the providers are understandably concerned. They've got shareholders, they've got fiduciary duties to their shareholders, they've got to protect them. And one thing the general counsels do is then they try to minimize their risk. And they do that by, sometimes, litigating things more just to make sure that they've got a court order to cover them at every step of the way. And that will really slow us down.

Q On that last part, can you just clarify exactly what happened over the weekend with the provider or providers who you were saying were reluctant to comply? Were any providers actually refusing to comply? And did you lose intelligence because of that? If so, what then happened over the weekend to change their position? Because there's a difference between being reluctant and refusing to comply. So which was it?

SENIOR ADMINISTRATION OFFICIAL: My answer -- let me step back a second. Both [my colleague] and I -- step back even farther for a second. Keep in mind who we're up representing. I'm in the Department of Justice. I have attorneys working with me who appear before the FISA court. So we're sort of the lawyer part of this equation. [My colleague], of course, in the intelligence community and is the operator part of the equation. Both of us have to work together to get these warrants -- FISA orders -- and to implement the Protect America Act.

Last week -- over, actually, the last few weeks, both [my colleague] and I, and colleagues of ours, both in ODNI and DOJ, have been working very closely with general counsels offices in the various providers, because they've been asking about this looming potential expiration for some time and what its implications will be. And in terms of -- to answer your question, I'm basically going to stick with what's been made public. And there's actually been a pretty good record so far made public between the letter from the DNI and the AG, and then -- which came out Friday afternoon, I guess. And then there was a subsequent press release or statement the next day from DOJ and ODNI.

Bottom line is, as the AG and the DNI said in that letter, most providers were complying with requests for new surveillances. These are surveillances we wanted to go up on under the directives that continued in force after the expiration of the PAA, but we wanted to go up on new surveillances under those directives. Most providers were complying, but as of the time that we sent the letter, not all. And then soon after that -- we've been in intense discussion, back and forth, with a number of different parties, we achieved full compliance -- just with that, with the compliance with our request to go up on new surveillances under those PAA directives. However, they've made it very clear that this isn't a permanent situation, and they're concerned about it and they might -- they may well withdraw that cooperation if the situation doesn't get cleared up with permanent legislation.

Q So what intelligence was lost? You talked about the loss of intelligence. Can you quantify that? As Director McConnell did back in August, he gave very dramatic statements about 75 percent of the intelligence had been lost because of this one loophole. You know, this all seems kind of abstract -- the intelligence that had been lost. What does that actually mean?

SENIOR ADMINISTRATION OFFICIAL: Last summer was a more long-term development in

coming. This was an intense period over a week, so we were not up on the new surveillances that we needed to go up on. So we were not up on those. We had valid foreign intelligence reasons to want to be initiating surveillance on these activities. We were not able to do that because of this issue with the providers. So we lost that time period from when we would have initiated these new surveillances to the time period in which we were able to come back up on them.

It's important to note -- let me just add one asterisk here, though, which is, the act has expired. This was what we thought was the clearest part of the act. And we had talked -- [my colleague] and I had both talked up on the Hill in hearings about this -- and I saw articles quoting us about, oh, yes, we can do -- we think we can do surveillances; that's pretty clear under the statute; we think we'll be successful on that. We outlined we were very concerned about new providers, new directives, new activities, which we thought we may encounter some issues on.

So we still have that problem with the act expired. So in addition to a problem we thought we didn't have, where everyone said, oh, yes, you could do new surveillances under existing directives and authorizations, we found that that was called seriously into question. And we still have the other problem -- we have an expired act and we need those tools.

Q Just to be clear -- called into question by whom, the general counsels for these companies? I mean, they're coming back to -- corporate lawyers coming to you guys and telling you what the law says? Is that what you're saying?

SENIOR ADMINISTRATION OFFICIAL: I'll characterize my back-and-forth with them. They're raising questions, and they're saying, look, we've got an expired piece of legislation; it's not crystal clear, for instance, what [my colleague] just said about, can we use the directives that are in place -- they continue for a year after they are put in place -- can we use them not only as to the providers to whom those directives were directed, but to another provider? And you look at the Protect America Act; it doesn't -- it's not crystal clear on that. It's not clear at all about that. And there's, they think, a very strong argument in the other direction.

So these general counsels are doing their jobs. They're saying, wait a minute, is that potential liability? We've got billions of dollars in liability looming in the background here from -- that we haven't been immunized from. We're very worried about that. We're not seeing immunity coming down the road any time real soon. And you're asking us to do something that's not terribly clear under a statute that's expired, and I've got shareholders to whom I owe my first duty. So should I just go ahead and cooperate under your reading of the statute, Mr. Government, or should I be extra cautious and risk-averse, and challenge that directive, when you ask me to go up on a surveillance against a terrorist suspect overseas -- should I challenge it in the FISA court and then go through the steps of litigation that will keep us in the dark?

SENIOR ADMINISTRATION OFFICIAL: And it should escape nobody's notice, because it certainly didn't escape them in my conversations -- so you're saying that the Attorney General believes this is clear, and he believes that this is legal, and he believes that we can rely on this representation? It escapes nobody's notice that that resembles a certain situation in 2001 where they still have not received any relief from it.

Q At what point do you start to need new -- I realize that you've got existing directives that last for a year, it sounds like --

SENIOR ADMINISTRATION OFFICIAL: From when each of those directives expires.

Q Yes, but is there a period in the short-term where you're going to need new directives, or are all these things going to be -- are all the existing directives going to be sufficient for some period of time?

SENIOR ADMINISTRATION OFFICIAL: I do not expect the existing directives are sufficient for the future to do our mission. As to when I might need a new directive, I could get back to my office right now and have a phone call saying we've discovered that there's something going on, a communication path that we do not cover with the current existing directive to a provider, and we need to have a directive out to cover this situation.

Let me back up. We do not issue directives widely. We issue them because we have a specific mission need to issue them, and we have procedures in place, and we have compliance in place, and we have the technical means in place. We do not just mail directives to people. This is very technical, and it's very complex. And it's something that we roll out very carefully. We can go through a great detail of what we've done over the past six months in terms of compliance, in terms of reporting to Congress, in terms of oversight by multiple organizations, in terms of briefings to members of Congress and staff. So we've rolled this out extremely carefully. We want to make sure that we are in compliance, that we have the right procedures in place. So that is not a system by which we are just broadly doing something without making sure we have all those procedures in place before we act. But there's many scenarios I can envision where we would need new directives.

Q Can you say how many directives there are now?

SENIOR ADMINISTRATION OFFICIAL: No.

Q The situation you just laid out, just to be clear, of needing a new directive, that has not happened in the 10 days since the Protect America Act expired? You're saying that might happen in the next two minutes, but that has not happened yet?

SENIOR ADMINISTRATION OFFICIAL: That's correct.

Q And if you needed that new directive -- the FISA court would always still be available, right, in typical court order route?

SENIOR ADMINISTRATION OFFICIAL: Right. Okay, excellent. The answer is, no. And this question, if I may rephrase a little bit is, well, you could just use the FISA court. We've seen that debate out there -- you just go to the FISA court and get an order. Remember what [my colleague] described: Under the Foreign Intelligence Surveillance Act, we have to go to the FISA court and make a number of showings. One of those is a probable cause showing, under the Fourth Amendment.

These are not things that are done quickly, necessarily. This kind of gets back to the debate of last summer, before the Protect America Act expired, which was, do we take our operators, our linguists, our analysts -- we're always asked, do you have enough people who speak the right languages; do you have people who understand the cultures -- should I pull them off of their mission to write a thick application, court application, making this probable cause showing, and then go to court for individual surveillances on foreign targets abroad? We simply cannot do that as an intelligence community. Certainly that was part of the huge problem last summer, where we were caught where the law had not been updated.

Second, should we have to make that probable cause showing? If you're going to make that -- if you're going to import the probable cause showing that applies here in the United States, and require us to have that same level of information that we use to wiretap somebody here in the United States, or do a physical search of a U.S. citizen, that is not a minor thing to do. So if you're going to apply that to our foreign targets abroad, that's a huge shift in what we do as a community, and you're changing the level of intelligence information that I need to initiate surveillance on somebody abroad. You're essentially applying something derived from the Fourth Amendment to our foreign mission.

I think DOJ did about 2,000-something FISAs in 2006 --

SENIOR ADMINISTRATION OFFICIAL: Twenty-three hundred or so, something like that.

SENIOR ADMINISTRATION OFFICIAL: I don't think I -- I'm not giving out any information to suggest that maybe there's more than 2,300 targets globally that the United States may be interested in.

SENIOR ADMINISTRATION OFFICIAL: Let me just add to that, keep in mind, we can individualize orders with each target surveillance with the FISA court. The Protect America Act allows us to do some broader surveillances, and that's hugely important operationally. Also, keep in mind, we talk about this Fourth Amendment standard -- what that means is that we have to establish, to the satisfaction of a federal judge, the person we want to target is a foreign power or an agent of a foreign power.

Now, there are a lot of circumstances where we're going to want to target somebody overseas for a legitimate foreign intelligence purpose -- and under the Protect America Act, that's all we need -- we need to show there's a legitimate foreign intelligence purpose -- but we might not have that probable cause here. There are a lot of surveillances like that. And so we have to resort to the FISA court for any category of surveillances. We would take all those surveillances for which we can't meet that probable cause standard, and we just wouldn't be able to do them.

SENIOR ADMINISTRATION OFFICIAL: Yes. I mean, two points that are perfect examples -- and we were severely criticized in the congressional joint inquiry. One of those criticisms was, of course, over the Moussaoui case, and you can read all about the details in the back-and-forth of what was required to meet that standard -- how do we show he's an agent of a foreign power; what kind of information; can we produce that information? All of that back- and-forth.

If you're saying that that standard needs to be applied to our foreign targets overseas, you're going to see that type of Moussaoui back-and-forth in -- I mean, it's just not something that's feasible for us to be able to do our mission as it was structured in 1978.

Let me hit one other point, which is, while under FISA you have the emergency authorization process -- the Attorney General can initiate an emergency authorization, and then you have 72 hours where you have to go to the FISA court. So why can't you act quickly under the emergency authorization part of FISA? There is no free pass under FISA. An analyst in my community cannot just initiate surveillance of somebody. The way it works is, that analyst goes to their supervisor, goes to their supervisor, goes to their supervisor -- that goes over to the Department of Justice; they vet it; it is personally signed -- approved by the Attorney General, Deputy Attorney General or [my colleague]. If we get it wrong, there are certain penalties that kick in under FISA, if we thought we had probable cause, but it turns out somebody got the facts wrong. Depending on what happens, we may have certain penalties that we incur.

So the showing is the same. I can tell you from experience that the Attorney General, the Deputy Attorney General and the Assistant Attorney General for National Security do not just accept an incoming phone call from somebody who -- an analyst who gives them a little bit of information; they say, sure, go ahead, and we'll take 72 hours and kind of figure out what the real facts are. The statute is very clear. We have to make that showing before the Attorney General will give us the approval.

Q So, I mean, the Protect America Act could sort of obviate -- make FISA obsolete, because it will always be easier to do --

SENIOR ADMINISTRATION OFFICIAL: No, FISA is -- again, here in the United States, domestically, the Protect America Act, the Senate bill: court order, go through FISA if you're acting -- if you're targeting here in the United States, domestically. And broader, targeting a U.S. person anywhere in the world we now have to go to the FISA court. So, no, I still expect that we'll have large numbers of FISAs for our domestic mission.

Q Can you clarify, though, while with the law being expired, are you operating wholly under the Protect America Act, even though it has expired? Or do you revert back to rules from the preceding law? In this in-between period right now, what rule are you operating under?

SENIOR ADMINISTRATION OFFICIAL: Well, we have some of the Protect America Act, that portion that continues that we've described. So we hope that the act -- the authorities that have been issued and these directives, that people will continue to act under them. So we're acting under those.

To the extent there are new things, we're going to have to mitigate the problem and figure out ways to mitigate it. FISA is not a complete substitute. In many cases, it may not be much of a substitute at all. It's a problem right now. We're trying to figure out if I have other problems, how I would mitigate them.

Q And given the amount of thought that you described earlier has gone into this legislative debate, why is this issue of retroactive immunity coming to a head now? Why wasn't it contemplated and included in an earlier version?

SENIOR ADMINISTRATION OFFICIAL: Well, it's been a subject of debate since 2006.

SENIOR ADMINISTRATION OFFICIAL: Let me -- okay, in the summer the Director of National Intelligence, he had his three principles I outlined; you can see the statements on our website, they're all out there. And those were his three principles: court order for targeting an American; no court order for doing our foreign intelligence to target overseas targets; and three, protection, both prospective and retroactive, and an ability to compel the help that we need.

It was determined in the situation that we were in, in the end of July, and the gravity of the situation, that the Congress was not going to be able to address this issue of retroactive liability protection. The DNI discussed this in a statement of, I believe, August 2nd or August 3rd, where he certainly had the strong belief that this was going to be addressed in September of 2007, and that was his understanding. So this has been discussed all the way going back to 2006. And the Senate has addressed in a very strong fashion.

Q On lost intelligence, could you just be a little bit more specific, because when people hear that as evidence that America is less safe, they want to know -- are we talking emails? What was lost? Is it that you lost intelligence, or you lost the ability to listen or monitor, and so some intelligence may have been lost? Can you -- is there any way -- because that goes to the heart of the question: Is America less safe? What intelligence -- when you say intelligence was lost last week, what are we talking about here?

SENIOR ADMINISTRATION OFFICIAL: Well, first, we had surveillances that we wanted to do, that we had valid reasons for doing the surveillances, that we were not able to do because the providers were not cooperating and because of the concern that they expressed --

Q A handful? A dozen? Ten? Any way at all to quantify for people, so they can have something? Because to hear that, obviously there's no, sort of, perspective here in terms of what this intelligence -- lost intelligence is.

SENIOR ADMINISTRATION OFFICIAL: Sure. It's very difficult for me to quantify. I mean, I have a number of indications -- I'm actually trying to get some of that additional information right now. I can't give you -- I mean, those numbers are all going to be highly sensitive, but I'll say this: All weekend, when the act expired, prior to the law being expired the intelligence agencies were very concerned. When they felt there was an impairment they got very concerned. And on a daily basis we were working this issue, I was contacting -- working with the Department of Justice -- they were working extraordinarily hard, as were the intelligence agencies. And the problem got worse over the week, as we identified new things that we needed to be doing. And certainly the intelligence agencies felt it was significant. They also felt that Congress needed to be notified.

So I'm not going to get into quantifying things, but if it was one piece of kind of unclear activity,

I don't think I would have seen the same concern from the intelligence agencies. I'm going to rely on their judgment, but they certainly felt it was a significant impairment and they certainly advised me that the Congress needed to be notified. And I don't think they would have done that if they didn't feel it was a significant impairment.

Q -- the letter that was put out today by Richard Clarke and Rand Beers and other intelligence officials sent to Director McConnell saying that he had distorted the debate through what they thought were misstatements about this supposed enhanced threat. The Democrats, of course, have had a field day, saying that the administration is crying wolf. And McConnell, himself, over the past two months has had to retract some statements about the Germany threat and others. Do you worry that when you make these statements, that the administration's credibility -- saying that we've lost intelligence, that we are in a more vulnerable position -- that some people just may not believe you?

SENIOR ADMINISTRATION OFFICIAL: Well, I'll let Dana and Tony speak to administration issues. I will speak for the -- from the Director's perspective and the intelligence perspective. I've not heard anyone question the NIE of the summer that talks about the homeland threat, the public version of that that we talked about -- I think it was the July NIE key judgments are public. So maybe people want to debate that NIE, but it is -- as far as I know, it's been fairly widely accepted. I did not hear members of Congress questioning what the NIE said. I have not heard members questioning what the DNI has outlined, in terms of the situation with the leadership, in terms of reconstitution, in terms of space to train and operate.

He's talked about the fourth piece that they're missing, in terms of operative cells, as far as we're aware here domestically. As recently as his last open threat testimony, though, and in some of the discussions that he's had, he's talked very clearly about what they want to do, in terms of moving operatives out of where they are into Europe, without visas, and how you would look at infiltrating the United States, or carrying out an attack elsewhere. So he's been very clear on that. And we track these people through a number of these tools, as he's discussed. So I'm not sure where the credibility gap is. The Germany --

Q Well, that's why I asked --

SENIOR ADMINISTRATION OFFICIAL: Well, you made the statement about --

Q My question was probably unclear then. The letter today from Clarke, Beers, Suzanne Spaulding, was talking about questioning his statements about enhanced threat over FISA -- over the loss of intelligence, and saying that he has distorted that issue. I wasn't sure whether I was clear on my question.

SENIOR ADMINISTRATION OFFICIAL: Okay, well, I mean, I stand by his statements. He's concerned that we had a dynamic tool under the Protect America Act. We've talked about some of the examples of the information that we've gathered over the past six months. We think it's been very valuable information under the Protect America Act.

We do not have all of the tools that the Protect America Act provides available to us right now.

We had the issue of last week. We have, even on the things that we thought were most clear, we have people telling us, for now we will continue with those things. We don't have some of the new tools that we provide.

So from the Director's perspective, who is charged with providing warning of threats to the nation, he's concerned; he doesn't have these dynamic tools that he thinks he has. If people want to question that, that's certainly their right to do it, but I think it's well backed up by the evidence.

SENIOR ADMINISTRATION OFFICIAL: If I could just -- one last thing on this. Please go look at the joint Attorney General-DNI letter from last Friday. It's very thorough, and it's a very reasoned letter that's sort of making the point in measured terms what it is we're missing, and what the problem is that we're facing now that the act has expired. And people have suggested that maybe this was something that was playing to politics, but you've got to look at the context here.

This was, A, it was a letter that was in response to inquiries from the Hill. We got a letter -- the President received a letter from Chairman Reyes about this very issue, so he asked the AGG and the DNI to respond, so they did respond with this well-thought-out letter. The letter itself acknowledges that most of the providers were cooperating with our requests, but that not all were.

I can't remember the exact language, but they say that we're hopeful that we will continue with our further efforts, we'll be able to mitigate these concerns, so we make it clear that we're working on it. And then later on that evening, once we do get to full compliance, the DOJ and ODNI immediately notify the intelligence committees up on the Hill that we've got full compliance now on that one area. And then the next day we put out a statement. So I think that whole exercise shows --

Q How did you get to full compliance, by telling them they were home-free?

SENIOR ADMINISTRATION OFFICIAL: It was a back-and-forth engagement with the general counsels' offices, so that they got to the point where, as the announcement says, they were willing to comply with our requests, but there's no guarantee they'd continue to do so.

Q We'll cover your ass. (Laughter.)

SENIOR ADMINISTRATION OFFICIAL: Help us protect our security.

(END)