NSA OPENING STATEMENT SENATE JUDICIARY COMMITTEE OPEN HEARING ON MEDIA LEAKS 31 JULY 2013

<u>Introduction</u>

Mr. Chairman, Mr. Ranking member, members of the committee, thank you for the opportunity to join with my colleagues to brief the committee on issues **you've identified** in your invitation and opening remarks. I am privileged today to represent the work of thousands of NSA, intelligence community and law enforcement personnel who employ the authorities provided by the combined efforts of the Congress, Federal Courts and the Executive Branch.

For its part, NSA is necessarily focused on the generation of foreign intelligence but we have worked hard and long with counterparts across the US government and allies to **ensure that we "discover and connect the dots"** -- exercising <u>only those authorities</u> <u>explicitly granted to us</u> and taking care to ensure the protection of civil liberties and privacy.

Per your request, I will briefly describe how NSA implements the two NSA programs leaked to the media almost two months ago, to include their purpose and the controls imposed on their use — the so-called PRISM program authorized under section 702 of the FISA amendment act (FAA) and the so-called 215 program which authorizes the collection of telephone metadata.

Let me first say that these programs are distinguished *but complementary* with distinct purposes and oversight mechanisms. Neither of these programs was intended to stand alone, delivering singular results that tell the 'whole story' about a particular threat to our Nation or its allies.

I'll start with <u>Section 702 of the FISA</u>, which authorizes the targeting of non-U.S. persons abroad for foreign intelligence purposes such as counter-terrorism and counter-proliferation.

- Specifically, Section 702 authorizes the collection of communications for the purpose of Foreign Intelligence with the compelled assistance of an electronic communication service provider.
- Under this authority NSA can collect communications for foreign intelligence purposes
 <u>only</u> when the person who is the target of our collection is a foreigner who is
 reasonably believed to be outside the US.
- Section 702 *cannot* be used to intentionally target:

- o any US citizen or other US person,
- o any person known to be in the US,
- o OR a person outside the United States if the purpose is to target a person inside the United States

This program is also key to our counterterrorism efforts; information used in greater than 90% of the 54 disrupted terrorism events we have previously cited in public testimony was gained from section 702 authorities.

As one example, **we've** discussed the case of Najibullah Zazi. NSA analysts, leveraging section 702 to target the email of a Pakistan-based al-Qaida terrorist, discovered that he was communicating with someone about a plot involving explosives. NSA tipped this exchange to the FBI who confirmed that the communicant was actually Denver-based Zazi, who we know now was planning an imminent attack on the New York subway system. Without the tip from FAA 702, the plot may never have been uncovered.

The second program, which we undertake through court orders under **Section 215 of the Patriot Act**, authorizes the collection of telephone metadata only.

- It does not allow the government to listen to anyone's phone calls.
- This program was specifically developed to allow the USG to detect communications between known or suspected terrorists who are operating outside the U.S. who are communicating with potential operatives inside the U.S., a gap highlighted by the attacks of 9/11. *In a phrase this program is focused on detecting terrorist plots that cross the seam between foreign terrorist organizations and the US homeland.* We have previously cited in public testimony, that section 215 made a contribution to 12 of the 13 terror plots with a US nexus, amongst the 54 world-wide plots cited earlier.

On operational value:

In considering operational value, it is important to begin with an understanding of the problem the government is trying to solve.

- It is simply this: If we have intelligence indicating that a foreign-based terrorist organization is plotting an act of terror against the homeland, how would we determine whether there is, in fact, a connection between persons operating overseas and operatives within the US?
- Many will recall that the inability of the US intelligence community to make such a connection between 9/11 hijacker Al Midhar operating in California and an Al Qaeda safe house in Yemen, which was discussed by the 9/11 commission report.

 NSA had in fact collected the Yemen end of their communications but due to the nature of our collection, had no way of determining the number or the location of Al Midhar on the other end.

So the problem becomes, if you have <u>one</u> telephone number for a person you reasonably believe is plotting an act of terror against the homeland, how do you find possible connections to that number crossing the seam between the homeland and overseas?

In simple terms, you are looking for a needle, *in this case a number*, in a haystack. But not just any number. You want to make a focused query against a body of data that returns only those numbers that are connected to the one you have reasonable suspicion is connected to a terrorist group.

But unless you have the haystack – in this case all the records of who called whom – you cannot answer the question. The confidence you will have in any answers returned by your query is necessarily tied to whether the haystack constitutes a reasonably complete set of records and whether those records look back a reasonable amount of time to enable you to discover a connection between conspirators who might plan and coordinate across several years.

Hence "all" the records are necessary to connect the dots of an ongoing plot, sometimes in a time sensitive situation, even if only an extremely small fraction of them is ever determined to be the match you're looking for.

The authorities work in concert

As I mentioned at the outset, these authorities work together to enable our support to counter-terrorism. A counter-terrorism investigation is the product of many leads, a handful of which may prove to be decisive. It is impossible to know which tool is going to generate the decisive lead in any particular case. In some cases, the leads may corroborate a lead FBI is already following; in others, it may help them prioritize leads for further investigation; in still others it may yield a number that was previously unknown to them. These leads results in threat assessments, preliminary investigations and full investigations; in some cases, the data from the program yields no results, helping to disprove leads and conserve investigative resources. This is the way we would want these programs to work: adding dots, affirming them, connecting them, and in so doing contributing key pieces to the larger intelligence picture.

Using the Zazi case, once FBI confirmed Zazi's identity, they passed NSA his phone number, for which NSA then made a determination of "Reasonable Articulable Suspicion", and used the number to search the 215 database. Based on that search NSA analysts discovered a previously unknown number in communication with Zazi for a man named Adis Medunjanin. While FBI had previously been aware of Medunjanin, the direct and recent connection to Zazi as well as another us-based extremist focused

the **FBI's** attention on him as a key lead in the plot. as you know, both Zazi and Medunjanin have been convicted for their role in the plot.

Controls and Limitations:

The <u>limitations and controls</u> imposed on the use of both of these programs are significant.

For the 215 metadata these controls are laid out in the FISA **court's "primary order"** which the executive branch has declassified this morning so that it might provide **context for the court's "secondary order", leak**ed earlier in the press, but which only dealt with the collection of the data.

Under rules imposed by the Primary Order:

- The metadata acquired and stored under the 215 authority <u>may be queried</u> only when there is a <u>reasonable suspicion</u> based on specific facts that **a "selector"** which is typically a phone number—is associated with specific foreign terrorist organizations.
- Under rules approved by the court, only 22 people at NSA are allowed to approve the selectors used to initiate a search in this data base; all queries are audited; only seven positions at NSA (a total of 11 people) are authorized to release query results that are believed to be associated with persons in the US.
- Reports are filed with the court every 30 days that specify the number of selectors approved, and disseminations made to the FBI that contain numbers believed to be in the US.
- And, while the data acquired under this authority might theoretically be useful in other intelligence activities or law enforcement investigations, its use for any other purpose than that which I've described is prohibited.

With this capability, we are very mindful that we must use it conservatively and judiciously, in close concert with our law enforcement colleagues and focused on the seam between foreign terrorist groups and potential domestic actors.

 During 2012, we only initiated queries for information in this dataset using fewer than 300 unique selectors. The information returned from these queries only included phone numbers, not the content, identity, or location of the called or calling party. And in 2012, based on those fewer than 300 selectors, we provided a total of 12 reports to FBI, which altogether 'tipped' less than 500 numbers.

The 702 program operates under equally strict controls that, while ensuring our efforts are focused on the collection of foreign intelligence, specifically address how analysts should handle incidentally collected US person communications.

When NSA targets a terrorist overseas, they may sometimes communicate with persons in the US (anyone in the US, a US citizen or foreign person, is considered a US person). That's what we call "incidental collection."

If the case of a communication involving a US person, we have court approved minimization procedures that we must follow.

- This was the case with Najibullah Zazi. As I mentioned, we intercepted that communication using 702 collection by focusing on the Pakistani based al-Qa'ida terrorist.
- While it was not completely clear from the communication who Zazi was or where he was located, NSA analysts immediately tipped this exchange to the FBI who confirmed that Zazi was in fact in Denver and subsequently acquired a warrant to target and access the content of his communications.
- Without that initial 702 tip from NSA, which came as a result of targeting an al-Qa'ida terrorist located overseas, the plot may never have been discovered.
- This tip was handled in complete accordance with the applicable minimization procedures which authorized NSA to disseminate information of or concerning a US person if the US person information is necessary to understand or assess foreign intelligence information.
- Finally, NSA cannot reverse target, i.e. target a foreign person overseas if the intent is to target the communications of a person in the US.

We do of course have tools that allow analysts to conduct focused searches of our holdings and listen to the content of legally acquired collection concerning foreign intelligence targets. Given that these communications have been shown to bear on our foreign intelligence mission, we must and do review them. But the purpose is to glean foreign intelligence and the rules for protecting the identities and communications of US persons are both clear and followed.

Looking forward:

Policy makers across the executive and legislative branches will ultimately decide whether we want to sustain or dispense with a tool designed to detect terrorist plots across the seam between foreign and domestic domains. Different implementations of the program can address the need, but each should be scored against several key attributes:

- Privacy concerns must be addressed through controls and accountability;
- It should be possible to make queries in a timely manner so that, in the most demanding case, results can support disruption of imminent plots;
- The database must be reasonably complete across providers and time to yield so that we can have confidence in the answers it yields about whether there is, or is not, a terrorist plot in play; and

• The data architecture is constructed in a manner that allows efficient follow-up queries to any selector that shows connections to other numbers of legitimate relevance to an ongoing plot.

Conclusion

Our primary responsibility is to defend the Nation. The programs we are discussing today are a core part of those efforts. We use them to protect the lives of Americans and our allies and partners worldwide.

Over 100 nations are capable of collecting Signals Intelligence or operating a lawful intercept capability that enable them to monitor communications.

- I think our Nation is amongst the best at protecting our privacy and civil liberties.
- We look forward to the discussions here and, if necessary, at classified sessions
 to more fully explore your questions BUT I note that the leaks that have taken
 place thus far will cause serious damage to our intelligence capabilities.
- More to the point, the irresponsible release of classified information will have a long-term detrimental impact on the Intelligence Community's ability to detect and help deter future attacks.
- The men and women of NSA are committed to compliance with the law and the
 protection of privacy and civil liberties. The solutions they develop and the
 actions they take defend the Constitution and the American people, both their
 physical safety and their right to privacy. We train them from their first day at
 work and throughout their career.
- This is also true of contractors. The actions of one contractor should not tarnish all the contractors because they do great work for our nation, as well.
- Allegations that low level analysts at NSA can exercise independent discretion beyond these controls to target communications is simply wrong.

Finally, whatever further choices the Nation makes on this matter in consultation and collaboration across the three branches of government, NSA will faithfully implement them — in both spirit and mechanism. To do otherwise would be to fail in the only oath we take — to support and defend the Constitution of the United States — to include protection of both National Security and Civil Liberties.

Opening Statement of Deputy Attorney General James M. Cole Before the Senate Judiciary Committee, July 31, 2013, 9:00am

Thank you, Mr. Chairman, Mr. Ranking Member and members of the committee, for inviting us here to speak about the 215 business records program and section 702 of FISA. With these programs and other intelligence activities, we are constantly seeking to achieve the right balance between the protection of national security and the protection of privacy and civil liberties. We believe these two programs have achieved the right balance.

First of all, both programs are conducted under public statutes passed and later reauthorized by Congress. Neither is a program that has been hidden away or off the books. In fact, all three branches of government play a significant role in the oversight of these programs. The Judiciary – through the Foreign Intelligence Surveillance Court – plays a role in authorizing the programs and overseeing compliance; the Executive Branch conducts extensive internal reviews to ensure compliance; and Congress passes the laws, oversees our implementation of those laws, and determines whether or not the current laws should be reauthorized and in what form.

Let me explain how this has worked in the context of the 215 program. The 215 program involves the collection of metadata from telephone calls. These are

telephone records maintained by the phone companies. They include the number a call was dialed from, the number the call was dialed to, the date and time of the call, and the length of the call. The records do not include names or other personal identifying information, they do not include cell site or other location information, and they do not include the content of any phone calls. These are the kinds of records that under longstanding Supreme Court precedent are not protected by the Fourth Amendment.

The short court order you have seen published in the newspapers only allows the government to acquire the phone records; it does not allow the government to access or use them. The terms under which the government may access or use the records is covered by another, more detailed court order. That other court order provides that the government can only search the data if it has a "reasonable, articulable suspicion" that the phone number being searched is associated with certain terrorist organizations. The order also imposes numerous other restrictions on NSA to ensure that only properly trained analysts may access the data, and that they can only access it when the reasonable, articulable suspicion predicate has been met and documented. The documentation of the analyst's justification is important so that it can be reviewed by supervisors before the search and audited afterwards to ensure compliance.

In the criminal context, the government could obtain the same types of records with a grand jury subpoena, without going to court. But here, we go to the court approximately every 90 days to seek the court's authorization to collect the records. In fact, since 2006, the court has authorized the program on 34 separate occasions by 14 different judges. As part of that renewal process, we inform the court whether there have been any compliance problems, and if there have been, the court will take a very hard look and make sure we have corrected these problems. As we have explained before, the 11 judges on the FISC are far from a rubber stamp; instead, they review all of our pleadings thoroughly, they question us, and they don't approve the order until they are satisfied that we have met all statutory and constitutional requirements.

In addition to the Judiciary, Congress also plays a significant role in this program. The classified details of this program have been extensively briefed to both the Judiciary and Intelligence Committees and their staffs on numerous occasions. If there are any significant issues that arise with the 215 program, those would be reported to the two committees right away. Any significant interpretations of FISA by the Court would likewise be reported to the committees under our statutory obligation to provide copies of any FISC opinion or order that includes a significant interpretation of FISA, along with the accompanying court

documents. All of this reporting is designed to assist the two committees in performing their oversight role with respect to the program.

In addition, Congress plays a role in reauthorizing the provision under which the government has carried out this program since 2006. Section 215 of the PATRIOT Act has been renewed several times since the program was initiated – including most recently for an additional four years in 2011. In connection with the recent renewals of 215 authority, the government provided a classified briefing paper to the House and Senate Intelligence Committees to be made available to all Members of Congress. That briefing paper set out the operation of the program in detail, explained that the government and the FISC had interpreted section 215 to authorize the bulk collection of telephone metadata, and stated that the government was collecting such information. We also made offers to brief any member on the 215 program. The availability of the briefing paper and opportunity of an oral briefing were communicated through letters sent by the Chairs of the Intelligence Committees to all Members of Congress. Thus, although we could not talk publicly about the program at the time – since its existence was properly classified - the Executive Branch took all reasonably available steps to ensure that members of Congress were appropriately informed about the program when they renewed the 215 authority.

I understand that there have been recent proposals to amend section 215 authority to limit the bulk collection of telephone metadata. As the President has said, we welcome a public debate about how best to safeguard both our national security and the privacy of our citizens. Indeed, we will be considering in the coming days and weeks further steps to declassify information and help facilitate that debate. In the meantime, however, we look forward to working with the Congress to determine in a careful and deliberate way what tools can best secure the nation while also protecting our privacy interests.

Although my opening remarks have focused on the 215 program, we stand ready to take your questions on the 702 program. Thank you.