JOINT STATEMENT FOR THE RECORD BY

MICHAEL LEITER
DIRECTOR
NATIONAL COUNTERTERRORISM CENTER

AND

[redacted]
ASSOCIATE DEPUTY DIRECTOR FOR COUNTERTERRORISM
SIGNALS INTELLIGENCE DIRECTORATE
NATIONAL SECURITY AGENCY

BEFORE THE
HOUSE PERMANENT SELECT COMMITTEE ON INTELLIGENCE
CLOSED HEARING ON PATRIOT ACT REAUTHORIZATION
OCTOBER 21, 2009

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: ~~20320108~~

(U) Introduction

(U) Chairman Reyes, Ranking Member Hoekstra, distinguished members of the committee, thank you for the opportunity to discuss the importance of Section 215 of the USA Patriot Act of 2001 to our Nation's security.

(U) Value of Section 215 Authorities to National Security

(~~TS//SI//NF~~) As this Committee well knows, since the tragedy of 9/11, the Intelligence Community has developed an array of capabilities to detect, identify and disrupt terrorist plots against the United States and its interests. Detecting threats by exploiting terrorist communications has been, and continues to be, one of the critical tools in that fight. Above all else, it is imperative that we have a capability to rapidly identify any terrorist threats emanating from within the United States. As you will see in the Illustrations area below, the Section 215 Authorities played an important role in helping the Intelligence Community understand more fully the connections associated with now indicted Najibullah Zazi.

(~~TS//SI//NF~~) Members will recall that, prior to the attacks of 9/11, the NSA intercepted and transcribed seven calls from hijacker Khalid al-Mihdhar to a facility associated with an al Qa'ida safehouse in Yemen. However, NSA's access point overseas did not provide the technical data indicating where al-Mihdhar was calling from. Lacking the originating phone number, and hearing nothing in the content of those calls to suggest he was in the United States, NSA analysts concluded that al-Mihdhar was overseas. In fact, al-Mihdhar was calling from San Diego, California. According to the 9/11 Commission Report (pages 269-272):

> *"Investigations or interrogation of them [Khalid al-Mihdhar, etc], and investigation of their travel and financial activities could have yielded evidence of connections to other participants in the 9/11 plot. The simple fact of their detention could have derailed the plan. In any case, the opportunity did not arise."*[1]

The Business Records FISA program, operated in accordance with FISA Court authorization pursuant to Section 215, is specifically developed to close the gap that allowed al-Mihdhar to be plotting undetected within the United States while communicating with a known SIGINT terrorism target overseas.

(~~S//SI//NF~~) Section 215 of the USA Patriot Act allows the FISA Court to authorize the Intelligence Community to collect the vital information that closes the critical seam between foreign threats and domestic entities. In particular, it allows the IC to detect:

- Phone numbers within the United States calling targeted phone numbers associated with suspected foreign terrorists abroad;

- Targeted phone numbers tied to suspected foreign terrorists abroad calling phone numbers in the United States; and
- Connections concerning communications between entities within the United States tied to a suspected foreign terrorist abroad

~~(S//SI//NF)~~ In this context, the term "targeted number" refers to a number or other telephone identifier for which there exists Reasonable Articulable Suspicion (RAS) to believe the number is used by [redacted]

~~(TS//SI//NF)~~ The authority to collect information in bulk under Section 215 of the USA Patriot Act was first granted by the Foreign Intelligence Surveillance Court in May 2006 and has been renewed approximately every 90 days thereafter. The business records orders grant access to bulk telephony business records, or telephony metadata. "Telephony business records" or "telephony metadata" are simply technical terms that include the phone number that placed a call, the phone number at the receiving end of a call, when the phone call was placed, the duration of the call, and similar information about the call. Telephony business records do not include the content of any phone calls. In other words, the business records orders issued by the FISC do not authorize the collection of what is being said in any telephone calls.

(~~TS//SI//NF~~) NSA needs access to telephony business records in bulk[1] so that it can quickly identify the network of contacts that a targeted number is connected to, whenever a targeted number is detected. NSA identifies the network of contact by applying sophisticated analysis to this metadata. The more metadata NSA has access to, the higher the chances are that NSA can identify or discover the network of contacts linked to targeted numbers. Information discovered through its analysis of the bulk telephony business records is provided to the FBI, which is then responsible for further investigation of any potential terrorist threat.

(U) In sum, these authorities and capabilities are about rapidly identifying individuals like al-Mihdhar who might be operational in the United States today as well as their network of contacts. The IC requires the BR FISA program to close the seam between foreign intelligence knowledge of threats and persons who may be connected to those threats in the US.

Illustrations of Sec 215 authorities and NSA capabilities in action

(~~TS//SI//NF~~) The foregoing discussion is not hypothetical. As of October 1, 2009, NSA has provided 295 reports to the FBI, CIA and NCTC containing telephone numbers in contact with numbers associated [redacted] Upon receipt of the reporting from NSA, the FBI sent investigative leads to relevant FBI Field

[1] ~~(TS//SI//NF)~~ The current Business Records Order authorizes NSA to collect the records for approximately [redacted]

Offices for investigative action. FBI representatives have indicated to NSA that the telephone contact reporting has provided leads and linkages to individuals in the United States with potential ties to terrorism who may not have otherwise been known to or identified by the FBI. In Calendar Year 2008, telephone numbers tipped from the NSA business records results either added value or led to:

- the opening of over 240 Threat Assessments
- the opening of over 100 Preliminary Investigations
- the opening of approximately 15 Full Investigations
- 180 National Security Letters issued.

~~(TS//SI//NF)~~ NSA tips derived from the Agency's analysis of BR FISA telephony metadata have contributed directly to the following specific cases.

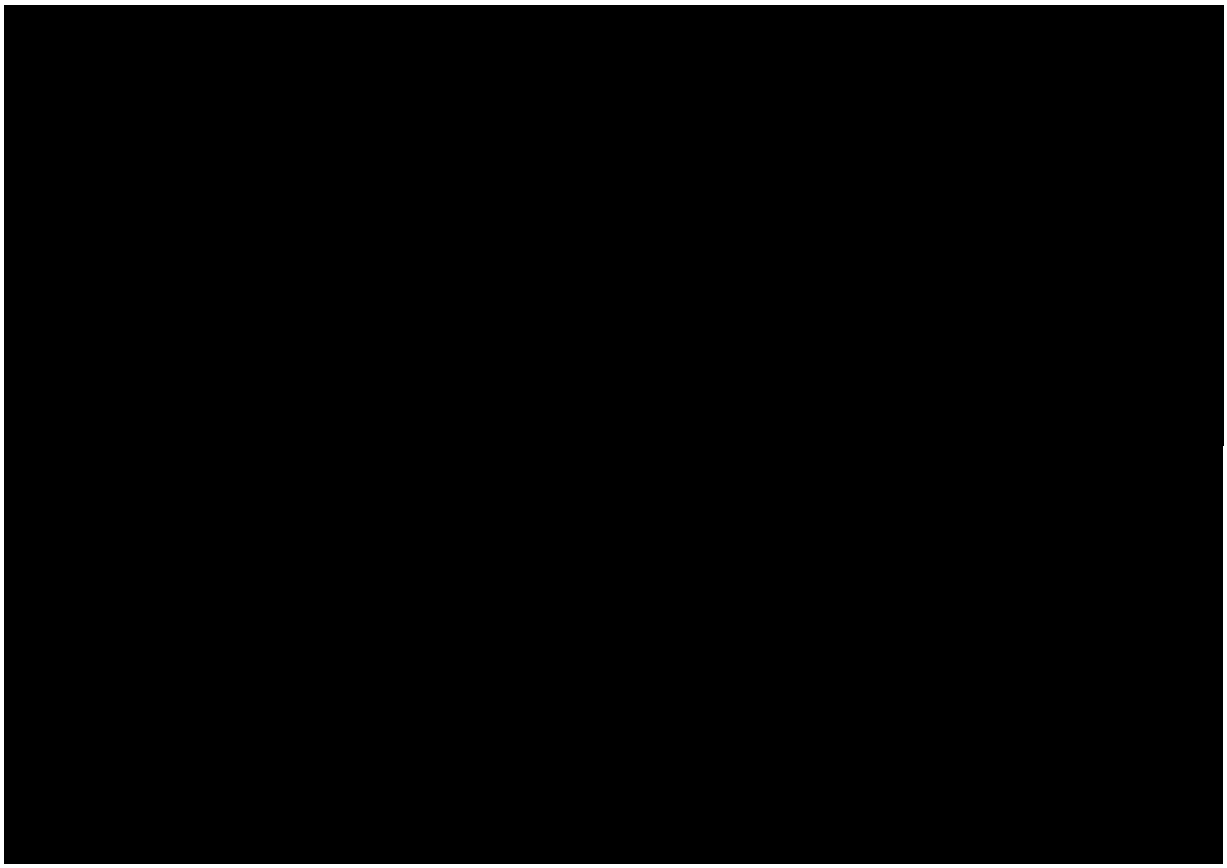
~~(TS//SI//NF)~~ **Investigation of Najibullah Zazi**. Now indicted, the Intelligence Community assesses that Najibullah Zazi -- in consultation with or under the guidance of a Pakistan-based al Qa'ida associate -- was conspiring to use Improvised Explosive Devices in the United States. BR FISA metadata played an important role in helping the IC understand more fully the range of Zazi's connections.

(TS//SI//NF) On September 6, 2009, using authorities under the FISA Amendments Act (FAA), NSA intercepted a coded email discussion between an al Qa'ida-associated email account previously accessed in Pakistan and an unknown account. NSA analysts quickly determined that the unknown account might be located in the United States and conveyed this information to the FBI in order that the FBI could obtain FISA coverage of the suspected US-based account. Through the FBI-obtained FISA, it was determined that the user of the account and an associated telephone number was Najibullah Zazi. Further investigation revealed Zazi's presence in Colorado. The FBI passed Zazi's mobile telephone number to NSA on the evening of 9-10 September.

~~(TS//SI//NF)~~ Shortly after receipt of Zazi's telephone number from FBI—and at approximately the same time that Zazi had obtained a one-way car rental from Colorado to New York City and had begun driving to New York—NSA issued a Business Records FISA metadata report on domestic and foreign contacts of that telephone. Among those contacts identified was a phone later confirmed as belonging to a key Zazi associate Adis Medunjanin. This was the FBI's first intelligence information about Medunjanin's telephone number and the contact corroborated other early information about Medunjanin's relationship with Zazi. It also magnified concerns about that relationship because, in that same report, NSA contextualized the Medunjanin phone as being in direct contact with three telephones (two domestic and one foreign) used by another extremist currently targeted in a priority FBI CT investigation. This detail, available only at the "second hop"[2] and only visible due to the blending of BR FISA and SIGINT data, quickly identified the Medunjanin number as a priority lead for the FBI. The detection

[2] ~~(S//SI//NF)~~ Second Hop: if the analysts submit a particular telephone number as a query, the database is designed to return any other telephone numbers that have called, or been called by, that number. This query process can be repeated for each of the returned numbers as well, generating information about communications two or three steps removed from the original number.

and alert of the Medunjanin connection was achieved through the agility of the BR FISA program. It provided timely, key information that was unavailable through any other sources and significantly accelerated and focused the investigation.



(~~TS//SI//NF~~) While these Business Records FISA successes are significant, the true value of the program to the nation is that it strengthens the Intelligence Community's early warning system for the detection of terrorists and discovery of plots. NSA monitors terrorist communications around the world on a broad scale. The nation requires a SIGINT system that will flash bright [redacted] ever there is an indication of a threat to the US Homeland. There is no doubt that [redacted] continues their aspirations and attempts to achieve another spectacular attack in the United States. The Business Records FISA program is a strategic program for the nation, connecting the nation's counterterrorism capabilities.

(~~TS//SI//NF~~) The Business Records FISC Order

(~~TS//SI//NF~~) As provided in the BR FISA Order, NSA's access to and use of BR FISA metadata records is governed by established minimization procedures. As the Committee is aware by way of previous written notification, on January 9, 2009, in the course of a regular review and discussion with NSA, the Department of Justice (DoJ) with NSA assistance identified what was ultimately determined to be an incident of non-compliance with the Order. Subsequently on January 15, 2009, DoJ filed a preliminary notice of non-compliance with the FISC.

(U//~~FOUO~~) In response to the Government's compliance notice, on January 28, 2009, the Court directed the Government to file a brief and supporting documentation describing the non-compliance matter. The Government's response to the order was filed with the FISC on February 17, 2009. On February 25, 2009, written notification of the matter was provided to the Committee.

(~~TS//SI//NF~~) On March 2, 2009, the FISC issued an Order restricting NSA's access to the metadata for intelligence purposes except upon Court approval on a case-by-case basis, with an exigency provision allowing for access when immediate access was necessary to protect against an imminent threat to human life. The Court also directed the Government to make certain filings: a declaration by at least the FBI Director describing the value of the metadata to national security, the results of the NSA end-to-end system engineering and process reviews, a statement concerning remedial efforts relating to matters of non-compliance and minimization and oversight procedures proposed in the event the Court were to determine to allow resumption of regular access to the BR metadata.

(U//~~FOUO~~) As the Committee has been made aware, these matters were given the utmost attention and addressed through changes in processes and implementation of FISC requirements during the ensuing months. In addition, and as further demonstration of NSA's commitment to a more robust compliance regime, NSA established a Director of Compliance with authority to develop, implement, and monitor a comprehensive compliance program that would complement and reinforce the intelligence oversight program carried out by the NSA/CSS Inspector General and the oversight responsibilities of the NSA/CSS General Counsel. This program is intended to integrate compliance strategies and activities across NSA/CSS's mission, technology and policy organizations; ensure a robust compliance training and education program; and maintain and report on a comprehensive status of mission compliance at NSA/CSS, including performing trend analysis and ensuring prompt corrective actions.

(~~TS//SI//NF~~) On September 3, 2009, after receiving extensive demonstrations and briefings regarding the BR FISA program, the FISC signed the Renewal Order for BR FISA. The order, which will remain in effect through October 30, 2009, restores to NSA the authority to make Reasonable Articulable Suspicion (RAS) determinations as to whether specific telephone identifiers may be used as "seeds" for querying against the BR FISA metadata. The signing of the renewal order is viewed as an indication that NSA is regaining the Court's confidence in its ability to safeguard US Person privacy while using BR FISA data for vital national security missions.

(~~TS//SI//NF~~) In conclusion, the BR FISA program provides a vital capability to the Intelligence Community. Recognizing that the program has implications for the privacy interests of US Person data, extensive policies, safeguards, and reviews have been enacted by the FISC, DOJ, DNI and NSA. 9/11 taught us that applying lead information from foreign intelligence in a comprehensive and systemic fashion is

required to protect the homeland. The Business Records FISA program operated under Section 215 of the USA Patriot act covers a critical seam in our defense against terrorism.