



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

February 2, 2011

The Honorable Dianne Feinstein  
Chairman  
The Honorable Saxby Chambliss  
Vice Chairman  
Select Committee on Intelligence  
United States Senate  
Washington, DC 20510

Dear Madam Chairman and Mr. Vice Chairman:

~~(TS)~~ Please find enclosed an updated document that describes the bulk collection programs conducted under Section 215 of the PATRIOT Act (the "business records" provision of the Foreign Intelligence Surveillance Act (FISA)) and Section 402 of FISA (the "pen/trap" provision). The Department and the Intelligence Community jointly prepared the enclosed document that describes these two bulk collection programs, the authorities under which they operate, the restrictions imposed by the Foreign Intelligence Surveillance Court, the National Security Agency's record of compliance, and the importance of these programs to the national security of the United States.

~~(TS)~~ We believe that making this document available to all Members of Congress, as we did with a similar document in December 2009, is an effective way to inform the legislative debate about reauthorization of Section 215. However, as you know, it is critical that Members understand the importance to national security of maintaining the secrecy of these programs, and that the SSCI's plan to make the document available to other Members is subject to the strict rules set forth below.

~~(TS)~~ Like the document provided to the Committee on December 13, 2009, the enclosed document is being provided on the understanding that it will be provided only to Members of Congress (and cleared SSCI, Judiciary Committee, and leadership staff), in a secure location in the SSCI's offices, for a limited time period to be agreed upon, and consistent with the rules of the SSCI regarding review of classified information and non-disclosure agreements. No

~~Classified by: Assistant Attorney General, NSD~~

~~Reason: 1.4(c)~~

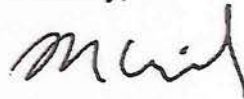
~~Declassify on: February 2, 2036~~

The Honorable Dianne Feinstein  
The Honorable Saxby Chambliss  
Page Two

photocopies may be made of the document, and any notes taken by Members may not be removed from the secure location. We further understand that SSCI staff will be present at all times when the document is being reviewed, and that Executive Branch officials will be available nearby during certain, pre-established times to answer questions should they arise. We also request your support in ensuring that the Members are well informed regarding the importance of this classified and extremely sensitive information to prevent any unauthorized disclosures resulting from this process. We intend to provide the same document to the House Permanent Select Committee on Intelligence (HPSCI) under similar conditions, so that it may be made available to the Members of the House, as well as cleared leadership, HPSCI and House Judiciary Committee staff.

(U) We look forward to continuing to work with you and your staff as Congress continues its deliberations on reauthorizing the expiring provisions of the USA PATRIOT Act.

Sincerely,



Ronald Weich  
Assistant Attorney General

Enclosure



U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

February 2, 2011

The Honorable Mike Rogers  
Chairman  
The Honorable C.A. Dutch Ruppersberger  
Ranking Minority Member  
Permanent Select Committee on Intelligence  
U.S. House of Representatives  
Washington, DC 20515

Dear Mr. Chairman and Congressman Ruppersberger:

~~(TS)~~ Please find enclosed an updated document that describes the bulk collection programs conducted under Section 215 of the PATRIOT Act (the "business records" provision of the Foreign Intelligence Surveillance Act (FISA)) and Section 402 of FISA (the "pen/trap" provision). The Department and the Intelligence Community jointly prepared the enclosed document that describes these two bulk collection programs, the authorities under which they operate, the restrictions imposed by the Foreign Intelligence Surveillance Court, the National Security Agency's record of compliance, and the importance of these programs to the national security of the United States.

~~(TS)~~ We believe that making this document available to all Members of Congress, as we did with a similar document in December 2009, is an effective way to inform the legislative debate about reauthorization of Section 215. However, as you know, it is critical that Members understand the importance to national security of maintaining the secrecy of these programs, and that the HPSCI's plan to make the document available to other Members is subject to the strict rules set forth below.

~~(TS)~~ Like the document provided to the Committee on December 13, 2009, the enclosed document is being provided on the understanding that it will be provided only to Members of Congress (and cleared HPSCI, Judiciary Committee, and leadership staff), in a secure location in the HPSCI's offices, for a limited time period to be agreed upon, and consistent with the rules of the HPSCI regarding review of classified information and non-disclosure agreements. No

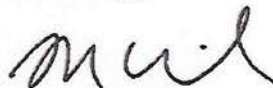
~~Classified by: Assistant Attorney General, NSD  
Reason: 1.4(c)  
Declassify on: February 2, 2036~~

The Honorable Mike Rogers  
The Honorable C.A. Dutch Ruppersberger  
Page Two

photocopies may be made of the document, and any notes taken by Members may not be removed from the secure location. We further understand that HPSCI staff will be present at all times when the document is being reviewed, and that Executive Branch officials will be available nearby during certain, pre-established times to answer questions should they arise. We also request your support in ensuring that the Members are well informed regarding the importance of this classified and extremely sensitive information to prevent any unauthorized disclosures resulting from this process. We intend to provide the same document to the Senate Select Committee on Intelligence (SSCI) under similar conditions, so that it may be made available to the Members of the Senate, as well as cleared leadership, SSCI and Senate Judiciary Committee staff.

(U) We look forward to continuing to work with you and your staff as Congress continues its deliberations on reauthorizing the expiring provisions of the USA PATRIOT Act.

Sincerely,



Ronald Weich  
Assistant Attorney General

Enclosure

~~(TS//SI//NF)~~ **Report on the National Security Agency's Bulk Collection Programs  
for USA PATRIOT Act Reauthorization**

(U) THE INFORMATION CONTAINED IN THIS REPORT DESCRIBES SOME OF THE MOST SENSITIVE FOREIGN INTELLIGENCE COLLECTION PROGRAMS CONDUCTED BY THE UNITED STATES GOVERNMENT. THIS INFORMATION IS HIGHLY CLASSIFIED AND ONLY A LIMITED NUMBER OF EXECUTIVE BRANCH OFFICIALS HAVE ACCESS TO IT. PUBLICLY DISCLOSING ANY OF THIS INFORMATION WOULD BE EXPECTED TO CAUSE EXCEPTIONALLY GRAVE DAMAGE TO OUR NATION'S INTELLIGENCE CAPABILITIES AND TO NATIONAL SECURITY. THEREFORE IT IS IMPERATIVE THAT ALL WHO HAVE ACCESS TO THIS DOCUMENT ABIDE BY THEIR OBLIGATION NOT TO DISCLOSE THIS INFORMATION TO ANY PERSON UNAUTHORIZED TO RECEIVE IT.

**Key Points**

- (U) Section 215 of the USA PATRIOT Act, which expires at the end of February 2011, allows the government, upon approval of the Foreign Intelligence Surveillance Court ("FISA Court"), to obtain access to certain business records for national security investigations;
- (U) Section 402 of the Foreign Intelligence Surveillance Act ("FISA"), which is not subject to a sunset, allows the government, upon approval of the FISA Court, to install and use a pen register or trap and trace ("pen/trap") device for national security investigations;
- ~~(TS//SI//NF)~~ These authorities support two sensitive and important intelligence collection programs. These programs are authorized to collect in bulk certain dialing, routing, addressing and signaling information about telephone calls and electronic communications, such as the telephone numbers or e-mail addresses that were communicating and the times and dates but not the content of the calls or e-mail messages themselves;
- ~~(TS//SI//NF)~~ Although the programs collect a large amount of information, the vast majority of that information is never reviewed by any person, because the information is not responsive to the limited queries that are authorized for intelligence purposes;
- ~~(TS//SI//NF)~~ The programs are subject to an extensive regime of internal checks, particularly for U.S. persons, and are monitored by the FISA Court and Congress;
- ~~(TS//SI//NF)~~ Although there have been compliance problems in recent years, the Executive Branch has worked to resolve them, subject to oversight by the FISA Court; and
- ~~(TS//SI//NF)~~ The National Security Agency's (NSA) bulk collection programs provide important tools in the fight against terrorism, especially in identifying terrorist plots against the homeland. These tools are also unique in that they can produce intelligence not otherwise available to NSA.

~~Derived From: NSA/CSSM 1-52~~

~~Dated: 20070108~~

~~Declassify On: 20360101~~

## Background

~~(TS//SI//NF)~~ 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 effort. Above all else, it is imperative that we have a capability to rapidly identify any terrorist threats emanating from within the United States.

~~(TS//SI//NF)~~ 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 the location from where al-Mihdhar was calling. Lacking the originating phone number, 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."*

~~(TS//SI//NF)~~ Today, under FISA Court authorization pursuant to the "business records" authority of the FISA (commonly referred to as "Section 215"), the government has developed a program to close the gap that allowed al-Mihdhar to plot undetected within the United States while communicating with a known terrorist overseas. This and similar programs operated pursuant to FISA, including exercise of pen/trap authorities, provide valuable intelligence information.

(U) Absent legislation, Section 215 will expire on February 28, 2011, along with the so-called "lone wolf" provision and roving wiretaps (which this document does not address). The pen/trap authority does not expire.

~~(TS//SI//NF)~~ The Section 215 and pen/trap authorities are used by the U.S. Government in selected cases to acquire significant foreign intelligence information that cannot otherwise be acquired either at all or on a timely basis. Any U.S. person information that is acquired is subject to strict, court-imposed restrictions on the retention, use, and dissemination of such information and is also subject to strict and frequent audit and reporting requirements.

~~(TS//SI//NF)~~ The largest and most significant use of these authorities is to support two important and highly sensitive intelligence collection programs under which NSA collects and analyzes large amounts of transactional data obtained from certain telecommunications service providers in the United States. [REDACTED]

[REDACTED] Although these programs have been briefed to the Intelligence and Judiciary Committees, it is important that other Members of Congress have access to information about these two programs when considering reauthorization of the expiring

PATRIOT Act provisions. The Executive Branch views it as essential that an appropriate statutory basis remains in place for NSA to conduct these two programs.

**Section 215 and Pen-Trap Collection**

~~(TS//SI//NF)~~ Under the program based on Section 215, NSA is authorized to collect from certain telecommunications service providers certain business records that contain information about communications between two telephone numbers, such as the date, time, and duration of a call. There is no collection of the content of any telephone call under this program, and under longstanding Supreme Court precedent the information collected is not protected by the Fourth Amendment. In this program, court orders (generally lasting 90 days) are served on [REDACTED] telecommunications companies [REDACTED]

[REDACTED] The orders generally require production of the business records (as described above) relating to substantially all of the telephone calls handled by the companies, including both calls made between the United States and a foreign country and calls made entirely within the United States.

~~(TS//SI//NF)~~ Under the program based on the pen/trap provision in FISA, the government is authorized to collect similar kinds of information about electronic communications – such as “to” and “from” lines in e-mail, certain routing information, and the date and time an e-mail is sent – excluding the content of the e-mail and the “subject” line. Again, this information is collected pursuant to court orders (generally lasting 90 days) and, under relevant court decisions, is not protected by the Fourth Amendment.

~~(TS//SI//NF)~~ Both of these programs operate on a very large scale. [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

However, as described below, only a tiny fraction of such records are ever viewed by NSA intelligence analysts.

**Checks and Balances**

FISA Court Oversight

~~(TS//SI//NF)~~ To conduct these bulk collection programs, the government has obtained orders from several different FISA Court judges based on legal standards set forth in Section 215 and the FISA pen/trap provision. Before obtaining any information from a telecommunications service provider, the government must establish, and the FISA Court must conclude, that the information is relevant to an authorized investigation. In addition, the government must comply with detailed “minimization procedures” required by the FISA Court that govern the retention and dissemination of the information obtained. Before NSA analysts may query bulk records, they must have reasonable articulable suspicion – referred to as “RAS” – that the number or e-mail address they submit is associated with [REDACTED]

[REDACTED] The RAS requirement is designed to protect against the indiscriminate querying of the collected data so that only information pertaining to one of the foreign powers listed in the relevant Court order [REDACTED] is provided to NSA personnel for further intelligence analysis. The bulk data collected under each program can be retained for 5 years.

Congressional Oversight

(U) These programs have been briefed to the Intelligence and Judiciary Committees, through hearings, briefings, and visits to NSA. In addition, the Intelligence and Judiciary Committees have been fully briefed on the compliance issues discussed below.

Compliance Issues

~~(TS//SI//NF)~~ In 2009, a number of technical compliance problems and human implementation errors in these two bulk collection programs were discovered as a result of Department of Justice (DOJ) reviews and internal NSA oversight. However, neither DOJ, NSA, nor the FISA Court has found any intentional or bad-faith violations. [REDACTED]

[REDACTED]

In accordance with the Court's rules, upon discovery, these inconsistencies were reported as compliance incidents to the FISA Court, which ordered appropriate remedial action. The FISA Court placed several restrictions on aspects of the business records collection program until the compliance processes were improved to its satisfaction. [REDACTED]

[REDACTED]

(U) The incidents, and the Court's responses, were also reported to the Intelligence and Judiciary Committees in great detail. The Committees, the Court and the Executive Branch have responded actively to the incidents. The Court has imposed safeguards that, together with greater efforts by the Executive Branch, have resulted in significant and effective changes in the compliance program.

(U) All parties will continue to report to the FISA Court and to Congress on compliance issues as they arise, and to address them effectively.



**Intelligence Value of the Collection**

~~(TS//SI//NF)~~ As noted, these two collection programs significantly strengthen the Intelligence Community's early warning system for the detection of terrorists and discovery of plots against the homeland. They allow the Intelligence Community to detect phone numbers and e-mail addresses within the United States that may be contacting targeted phone numbers and e-mail addresses associated with suspected foreign terrorists abroad and vice-versa; and entirely domestic connections between entities within the United States tied to a suspected foreign terrorist abroad. NSA needs access to telephony and e-mail transactional information in bulk so that it can quickly identify and assess the network of contacts that a targeted number or address is connected to, whenever there is RAS that the targeted number or address is associated with [REDACTED]

[REDACTED] Importantly, there are no intelligence collection tools that, independently or in combination, provide an equivalent capability.

~~(TS//SI//NF)~~ To maximize the operational utility of the data, the data cannot be collected prospectively once a lead is developed because important connections could be lost in data that was sent prior to the identification of the RAS phone number or e-mail address. NSA identifies the network of contacts by applying sophisticated analysis to the massive volume of metadata – but always based on links to a number or e-mail address which itself is associated with a counterterrorism target. (Again, communications metadata is the dialing, routing, addressing or signaling information associated with an electronic communication, but not content ) The more metadata NSA has access to, the more likely it is that NSA can identify, discover and understand the network of contacts linked to targeted numbers or addresses. Information discovered through NSA's analysis of the metadata is then provided to the appropriate federal national security agencies, including the FBI, which are responsible for further investigation or analysis of any potential terrorist threat to the United States.

\*\*\*\*\*

~~(TS//SI//NF)~~ In conclusion, the Section 215 and pen/trap bulk collection programs provide an important capability to the Intelligence Community. The attacks of 9/11 taught us that applying lead information from foreign intelligence in a comprehensive and systemic fashion is required to protect the homeland, and the programs discussed in this paper cover a critical seam in our defense against terrorism. Recognizing that the programs have implications for the privacy interests of U.S. person data, extensive policies, safeguards, and reviews have been enacted by the FISA Court, DOJ, ODNI and NSA.



U.S. Department of Justice  
Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

December 14, 2009

The Honorable Silvestre Reyes  
Chairman  
Permanent Select Committee on Intelligence  
United States House of Representatives  
HVC-304, The Capitol  
Washington, DC 20515

Dear Chairman Reyes:

~~(TS)~~ Thank you for your letter of September 30, 2009, requesting that the Department of Justice provide a document to the House Permanent Select Committee on Intelligence (HPSCI) that describes the bulk collection program conducted under Section 215 -- the "business records" provision of the Foreign Intelligence Surveillance Act (FISA). We agree that it is important that all Members of Congress have access to information about this program, as well as a similar bulk collection program conducted under the pen register/trap and trace authority of FISA, when considering reauthorization of the expiring USA PATRIOT Act provisions.

~~(TS)~~ The Department has therefore worked with the Intelligence Community to prepare the enclosed document that describes these two bulk collection programs, the authorities under which they operate, the restrictions imposed by the Foreign Intelligence Surveillance Court, the National Security Agency's record of compliance, and the importance of these programs to the national security of the United States. We believe that making this document available to all Members of Congress is an effective way to inform the legislative debate about reauthorization of Section 215 and any changes to the FISA pen register/trap and trace authority. However, as you know, it is critical that Members understand the importance to national security of maintaining the secrecy of these programs, and that the HPSCI's plan to make the document available to other Members is subject to strict rules.

~~Classified by: Assistant Attorney General, NSD  
Reason: 1.4(c)  
Declassify on: 11 December 2034~~

~~(TS)~~ Therefore, the enclosed document is being provided on the understanding that it will be provided only to Members of Congress (and cleared HPSCI, Judiciary Committee, and leadership staff), in a secure location in the HPSCI's offices, for a limited time period to be agreed upon, and consistent with the rules of the HPSCI regarding review of classified information and non-disclosure agreements. No photocopies may be made of the document, and any notes taken by Members may not be removed from the secure location. We further understand that HPSCI staff will be present at all times when the document is being reviewed, and that Executive Branch officials will be available nearby during certain, pre-established times to answer questions should they arise. We also request your support in ensuring that the Members are well informed regarding the importance of this classified and extremely sensitive information to prevent any unauthorized disclosures resulting from this process. We intend to provide the same document to the Senate Select Committee on Intelligence (SSCI) under similar conditions, so that it may be made available to the Members of the Senate, as well as cleared leadership, SSCI and Senate Judiciary Committee staff.

(U) Thank you again for your letter, and we look forward to continuing to work with you and your staff as Congress continues its deliberations on reauthorizing the expiring provisions of the USA PATRIOT Act.

Sincerely,



Ronald Weich  
Assistant Attorney General

~~(TS//SI//NF)~~ **Report on the National Security Agency's Bulk Collection Programs Affected by USA PATRIOT Act Reauthorization**

(U) THE INFORMATION CONTAINED IN THIS REPORT DESCRIBES SOME OF THE MOST SENSITIVE FOREIGN INTELLIGENCE COLLECTION PROGRAMS CONDUCTED BY THE UNITED STATES GOVERNMENT. THIS INFORMATION IS HIGHLY CLASSIFIED AND ONLY A LIMITED NUMBER OF EXECUTIVE BRANCH OFFICIALS HAVE ACCESS TO IT. PUBLICLY DISCLOSING ANY OF THIS INFORMATION WOULD BE EXPECTED TO CAUSE EXCEPTIONALLY GRAVE DAMAGE TO OUR NATION'S INTELLIGENCE CAPABILITIES AND TO NATIONAL SECURITY. THEREFORE IT IS IMPERATIVE THAT ALL WHO HAVE ACCESS TO THIS DOCUMENT ABIDE BY THEIR OBLIGATION NOT TO DISCLOSE THIS INFORMATION TO ANY PERSON UNAUTHORIZED TO RECEIVE IT.

Key Points

- ~~(TS//SI//NF)~~ Provisions of the USA PATRIOT Act affected by reauthorization legislation support two sensitive intelligence collection programs;
- ~~(TS//SI//NF)~~ These programs are authorized to collect in bulk certain dialing, routing, addressing and signaling information about telephone calls and electronic communications, such as the telephone numbers or e-mail addresses that were communicating and the times and dates but not the content of the calls or e-mail messages themselves;
- ~~(TS//SI//NF)~~ Although the programs collect a large amount of information, the vast majority of that information is never reviewed by anyone in the government, because the information is not responsive to the limited queries that are authorized for intelligence purposes;
- ~~(TS//SI//NF)~~ The programs are subject to an extensive regime of internal checks, particularly for U.S. persons, and are monitored by the Foreign Intelligence Surveillance Court ("FISA Court") and Congress;
- ~~(TS//SI//NF)~~ The Executive Branch, including DOJ, ODNI, and NSA, takes any compliance problems in the programs very seriously, and substantial progress has been made in addressing those problems. [REDACTED] and [REDACTED]
- ~~(TS//SI//NF)~~ NSA's bulk collection programs provide important tools in the fight against terrorism, especially in identifying terrorist plots against the homeland. These tools are also unique in that they can produce intelligence not otherwise available to NSA.

~~Classified by: Assistant Attorney General, NSD  
Reason: 1.4(c)  
Declassify on: 11 December 2034~~

## Background

~~(TS//SI//NF)~~ 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 effort. Above all else, it is imperative that we have a capability to rapidly identify any terrorist threats emanating from within the United States.

~~(TS//SI//NF)~~ Prior to the attacks of 9/11, the National Security Agency (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 the location from where al-Mihdhar was calling. Lacking the originating phone number, 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."*

~~(TS//SI//NF)~~ Today, under Foreign Intelligence Surveillance Court authorization pursuant to the "business records" authority of the Foreign Intelligence Surveillance Act (FISA) (commonly referred to as "Section 215"), the government has developed a program to close the gap that allowed al-Mihdhar to plot undetected within the United States while communicating with a known terrorism target overseas. This and similar programs operated pursuant to FISA provide valuable intelligence information.

(U) USA PATRIOT Act reauthorization legislation currently pending in both the House and the Senate would alter, among other things, language in two parts of FISA: Section 215 and the FISA "pen register/trap and trace" (or "pen-trap") authority. Absent legislation, Section 215 will expire on December 31, 2009, along with the so-called "lone wolf" provision and roving wiretaps (which this document does not address). The FISA pen-trap authority does not expire, but the pending legislation in the Senate and House includes amendments of this provision.

~~(TS//SI//NF)~~ The Section 215 and pen-trap authorities are used by the U.S. Government in selected cases to acquire significant foreign intelligence information that cannot otherwise be acquired either at all or on a timely basis. Any U.S. person information that is acquired is subject to strict, court-imposed restrictions on the retention, use, and dissemination of such information and is also subject to strict and frequent audit and reporting requirements.

~~(TS//SI//NF)~~ The largest and most significant uses of these authorities are to support two critical and highly sensitive intelligence collection programs under which NSA collects and analyzes large amounts of transactional data obtained from telecommunications providers [REDACTED]

[REDACTED] Although these programs have been briefed to

the Intelligence and Judiciary Committees, it is important that other Members of Congress have access to information about these two programs when considering reauthorization of the expiring PATRIOT Act provisions. The Executive Branch views it as essential that an appropriate statutory basis remains in place for NSA to conduct these two programs.

**Section 215 and Pen-Trap Collection**

~~(TS//SI//NF)~~ Under the program based on Section 215, NSA is authorized to collect from telecommunications service providers certain business records that contain information about communications between two telephone numbers, such as the date, time, and duration of a call. There is no collection of the content of any telephone call under this program, and under longstanding Supreme Court precedent the information collected is not protected by the Fourth Amendment. In this program, court orders (generally lasting 90 days) are served on [REDACTED] telecommunications companies [REDACTED]

[REDACTED] The orders generally require production of the business records (as described above) relating to substantially all of the telephone calls handled by the companies, including both calls made between the United States and a foreign country and calls made entirely within the United States.

~~(TS//SI//NF)~~ Under the program based on the pen-trap provisions in FISA, the government is authorized to collect similar kinds of information about electronic communications – such as “to” and “from” lines in e-mail and the time an e-mail is sent – excluding the content of the e-mail and the “subject” line. Again, this information is collected pursuant to court orders (generally lasting 90 days) and, under relevant court decisions, is not protected by the Fourth Amendment. [REDACTED]

~~(TS//SI//NF)~~ Both of these programs operate on a very large scale. [REDACTED]

## Checks and Balances

### FISA Court Oversight

~~(TS//SI//NF)~~ To conduct these bulk collection programs, the government has obtained orders from several different FISA Court judges based on legal standards set forth in Section 215 and the FISA pen-trap provision. Before obtaining any information from a telecommunication service provider, the government must establish, and the FISA Court must conclude, that the information is relevant to an authorized investigation. In addition, the government must comply with detailed "minimization procedures" required by the FISA Court that govern the retention and dissemination of the information obtained. Before an NSA analyst may query bulk records, they must have reasonable articulable suspicion – referred to as "RAS" – that the number or e-mail address they submit is associated with [REDACTED]

[REDACTED] The RAS requirement is designed to protect against the indiscriminate querying of the collected data so that only information pertaining to one of the foreign powers listed in the relevant Court order [REDACTED] is provided to NSA personnel for further intelligence analysis. There are also limits on how long the collected data can be retained (5 years in the Section 215 program, and 4½ years in the pen-trap program).

### Congressional Oversight

(U) These programs have been briefed to the Intelligence and Judiciary Committees, to include hearings, briefings, and, with respect to the Intelligence Committees, visits to NSA. In addition, the Intelligence Committees have been fully briefed on the compliance issues discussed below.

## Compliance Issues

~~(TS//SI//NF)~~ There have been a number of technical compliance problems and human implementation errors in these two bulk collection programs, discovered as a result of Department of Justice reviews and internal NSA oversight. However, neither the Department, NSA nor the FISA Court has found any intentional or bad-faith violations. The problems generally involved the implementation of highly sophisticated technology in a complex and ever-changing communications environment which, in some instances, resulted in the automated tools operating in a manner that was not completely consistent with the specific terms of the Court's orders. In accordance with the Court's rules, upon discovery, these inconsistencies were reported as compliance incidents to the FISA Court, which ordered appropriate remedial action. The incidents, and the Court's responses, were also reported to the Intelligence Committees in great detail. The Committees, the Court and the Executive Branch have responded actively to the incidents. The Court has imposed additional safeguards. In response to compliance problems, the Director of NSA also ordered "end-to-end" reviews of the Section 215 and pen-trap collection programs, and created a new position, the Director of Compliance, to help ensure the integrity of future collection. In early September of 2009, the Director of NSA made a presentation to the FISA Court about the steps taken to address the compliance issues. All

parties will continue to report to the FISA Court and to Congress on compliance issues as they arise, and to address them effectively.

**Intelligence Value of the Collection**

~~(TS//SI//NF)~~ As noted, these two collection programs significantly strengthen the Intelligence Community's early warning system for the detection of terrorists and discovery of plots against the homeland. They allow the Intelligence Community to detect phone numbers and e-mail addresses within the United States contacting targeted phone numbers and e-mail addresses associated with suspected foreign terrorists abroad and vice-versa; and connections between entities within the United States tied to a suspected foreign terrorist abroad. NSA needs access to telephony and e-mail transactional information in bulk so that it can quickly identify the network of contacts that a targeted number or address is connected to, whenever there is RAS that the number or address is associated with [REDACTED]

[REDACTED] Importantly, there are no intelligence collection tools that, independently or in combination, provide an equivalent capability.

~~(TS//SI//NF)~~ To maximize the operational utility of the data, the data cannot be collected prospectively once a lead is developed because important connections could be lost in data that was sent prior to the identification of the RAS phone number or e-mail address. NSA identifies the network of contacts by applying sophisticated analysis to the massive volume of metadata. (Communications metadata is the dialing, routing, addressing or signaling information associated with an electronic communication, but not content.). The more metadata NSA has access to, the more likely it is that NSA can identify or discover the network of contacts linked to targeted numbers or addresses. Information discovered through NSA's analysis of the metadata is then provided to the appropriate federal national security agencies, including the FBI, which are responsible for further investigation or analysis of any potential terrorist threat to the United States.

\*\*\*\*\*

~~(TS//SI//NF)~~ In conclusion, the Section 215 and pen-trap bulk collection programs provide a vital capability to the Intelligence Community. The attacks of 9/11 taught us that applying lead information from foreign intelligence in a comprehensive and systemic fashion is required to protect the homeland, and the programs discussed in this paper cover a critical seam in our defense against terrorism. Recognizing that the programs have implications for the privacy interests of U.S. person data, extensive policies, safeguards, and reviews have been enacted by the FISA Court, DOJ, ODNI and NSA.



~~TOP SECRET//SI//NOFORN~~

UNITED STATES  
FOREIGN INTELLIGENCE SURVEILLANCE COURT  
WASHINGTON, D. C.

---

IN RE APPLICATION OF THE FEDERAL  
BUREAU OF INVESTIGATION FOR AN  
ORDER REQUIRING THE PRODUCTION  
OF TANGIBLE THINGS FROM [REDACTED]

[REDACTED]

Docket Number: BR

13 - 8 0

---

PRIMARY ORDER

A verified application having been made by the Director of the Federal Bureau of Investigation (FBI) for an order pursuant to the Foreign Intelligence Surveillance Act of 1978 (the Act), Title 50, United States Code (U.S.C.), § 1861, as amended, requiring the

~~TOP SECRET//SI//NOFORN~~

Derived from: Pleadings in the above-captioned docket  
Declassify on: 12 April 2038

~~TOP SECRET//SI//NOFORN~~

production to the National Security Agency (NSA) of the tangible things described below, and full consideration having been given to the matters set forth therein, the Court finds as follows:

1. There are reasonable grounds to believe that the tangible things sought are relevant to authorized investigations (other than threat assessments) being conducted by the FBI under guidelines approved by the Attorney General under Executive Order 12333 to protect against international terrorism, which investigations are not being conducted solely upon the basis of activities protected by the First Amendment to the Constitution of the United States. [50 U.S.C. § 1861(c)(1)]

2. The tangible things sought could be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things. [50 U.S.C. § 1861(c)(2)(D)]

3. The application includes an enumeration of the minimization procedures the government proposes to follow with regard to the tangible things sought. Such procedures are similar to the minimization procedures approved and adopted as binding by the order of this Court in Docket Number [REDACTED] and its predecessors. [50 U.S.C. § 1861(c)(1)]

~~TOP SECRET//SI//NOFORN~~

Accordingly, the Court finds that the application of the United States to obtain the tangible things, as described below, satisfies the requirements of the Act and, therefore,

IT IS HEREBY ORDERED, pursuant to the authority conferred on this Court by the Act, that the application is GRANTED, and it is

FURTHER ORDERED, as follows:

(1)A. The Custodians of Records of [REDACTED] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata"<sup>1</sup> created by [REDACTED]

B. The Custodian of Records of [REDACTED]  
[REDACTED]  
[REDACTED] shall produce to NSA upon service of the appropriate secondary order, and continue production on an ongoing daily basis

---

<sup>1</sup> For purposes of this Order "telephony metadata" includes comprehensive communications routing information, including but not limited to session identifying information (e.g., originating and terminating telephone number, International Mobile Subscriber Identity (IMSI) number, International Mobile station Equipment Identity (IMEI) number, etc.), trunk identifier, telephone calling card numbers, and time and duration of call. Telephony metadata does not include the substantive content of any communication, as defined by 18 U.S.C. § 2510(8), or the name, address, or financial information of a subscriber or customer.

thereafter for the duration of this order, unless otherwise ordered by the Court, an electronic copy of the following tangible things: all call detail records or "telephony metadata" created by [REDACTED] for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. [REDACTED]

[REDACTED]

[REDACTED]

(2) With respect to any information the FBI receives as a result of this Order (information that is disseminated to it by NSA), the FBI shall follow as minimization procedures the procedures set forth in *The Attorney General's Guidelines for Domestic FBI Operations* (September 29, 2008).

(3) With respect to the information that NSA receives as a result of this Order, NSA shall strictly adhere to the following minimization procedures:

A. The government is hereby prohibited from accessing business record metadata acquired pursuant to this Court's orders in the above-captioned docket and its predecessors ("BR metadata") for any purpose except as described herein.

B. NSA shall store and process the BR metadata in repositories within secure networks under NSA's control.<sup>2</sup> The BR metadata shall carry unique markings such

---

<sup>2</sup> The Court understands that NSA will maintain the BR metadata in recovery back-up systems for mission assurance and continuity of operations purposes. NSA shall ensure that any access

that software and other controls (including user authentication services) can restrict access to it to authorized personnel who have received appropriate and adequate training with regard to this authority. NSA shall restrict access to the BR metadata to authorized personnel who have received appropriate and adequate training.<sup>3</sup>

Appropriately trained and authorized technical personnel may access the BR metadata to perform those processes needed to make it usable for intelligence analysis. Technical personnel may query the BR metadata using selection terms<sup>4</sup> that have not been RAS-approved (described below) for those purposes described above, and may share the results of those queries with other authorized personnel responsible for these purposes,

---

or use of the BR metadata in the event of any natural disaster, man-made emergency, attack, or other unforeseen event is in compliance with the Court's Order.

<sup>3</sup> The Court understands that the technical personnel responsible for NSA's underlying corporate infrastructure and the transmission of the BR metadata from the specified persons to NSA, will not receive special training regarding the authority granted herein.

[REDACTED]

but the results of any such queries will not be used for intelligence analysis purposes. An authorized technician may access the BR metadata to ascertain those identifiers that may be high volume identifiers. The technician may share the results of any such access, *i.e.*, the identifiers and the fact that they are high volume identifiers, with authorized personnel (including those responsible for the identification and defeat of high volume and other unwanted BR metadata from any of NSA's various metadata repositories), but may not share any other information from the results of that access for intelligence analysis purposes. In addition, authorized technical personnel may access the BR metadata for purposes of obtaining foreign intelligence information pursuant to the requirements of subparagraph (3)C below.

C. NSA shall access the BR metadata for purposes of obtaining foreign intelligence information only through contact chaining queries of the BR metadata as described in paragraph 17 of the Declaration of [REDACTED], attached to the application as Exhibit A, using selection terms approved as "seeds" pursuant to the RAS approval process described below.<sup>5</sup> NSA shall ensure, through adequate and

---

<sup>5</sup> For purposes of this Order, "National Security Agency" and "NSA personnel" are defined as any employees of the National Security Agency/Central Security Service ("NSA/CSS" or "NSA") and any other personnel engaged in Signals Intelligence (SIGINT) operations authorized pursuant to FISA if such operations are executed under the direction, authority, or control of the Director, NSA/Chief, CSS (DIRNSA). NSA personnel shall not disseminate BR metadata outside the NSA unless the dissemination is permitted by, and in accordance with, the requirements of this Order that are applicable to the NSA.

appropriate technical and management controls, that queries of the BR metadata for intelligence analysis purposes will be initiated using only a selection term that has been RAS-approved. Whenever the BR metadata is accessed for foreign intelligence analysis purposes or using foreign intelligence analysis query tools, an auditable record of the activity shall be generated.<sup>6</sup>

(i) Except as provided in subparagraph (ii) below, all selection terms to be used as "seeds" with which to query the BR metadata shall be approved by any of the following designated approving officials: the Chief or Deputy Chief, Homeland Security Analysis Center; or one of the twenty specially-authorized Homeland Mission Coordinators in the Analysis and Production Directorate of the Signals Intelligence Directorate. Such approval shall be given only after the designated approving official has determined that based on the factual and practical considerations of everyday life on which reasonable and prudent persons act, there are facts giving rise to a reasonable, articulable suspicion (RAS) that the selection term to be queried is associated with [REDACTED]


[REDACTED]

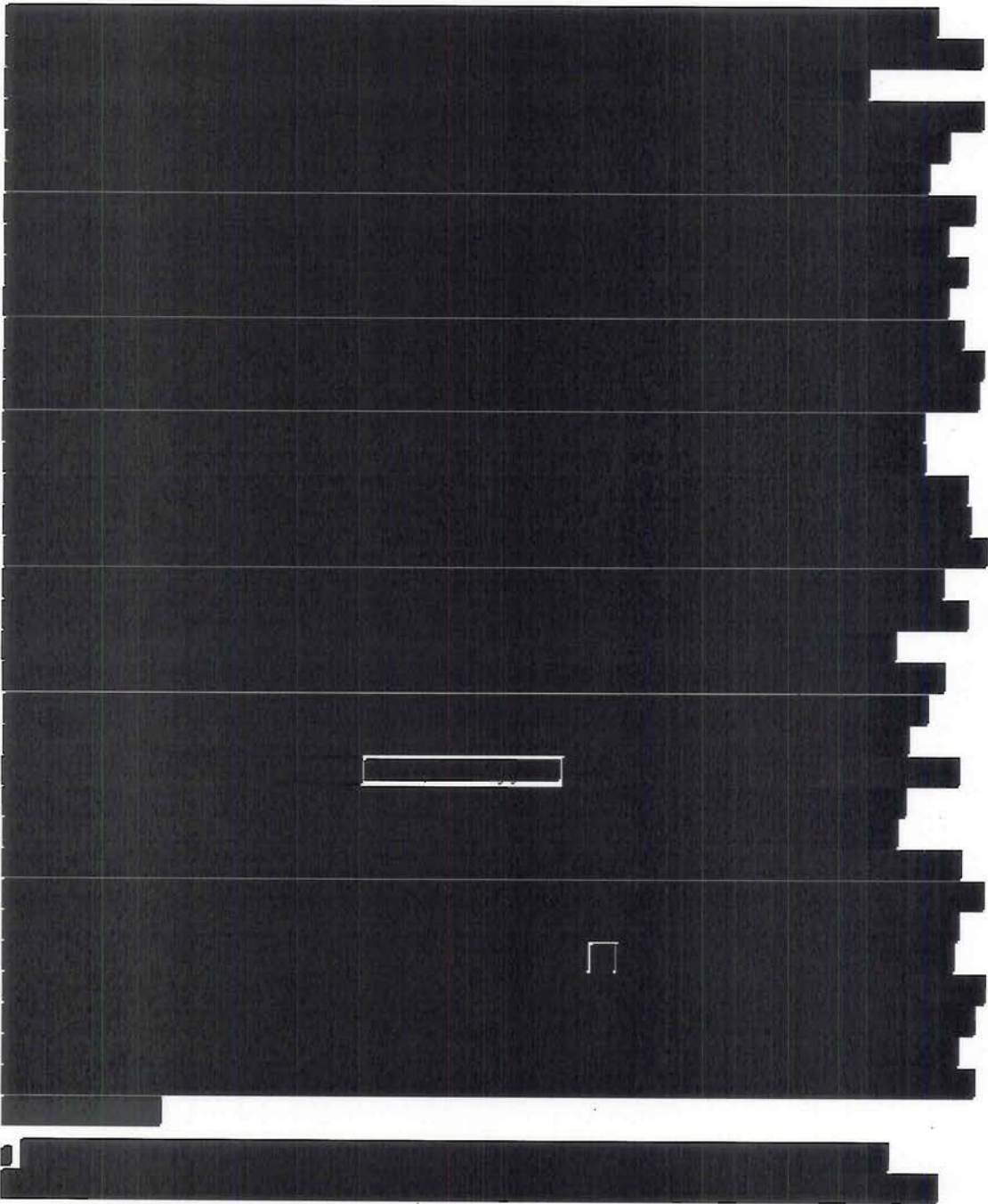
---

<sup>6</sup> This auditable record requirement shall not apply to accesses of the results of RAS-approved queries.

[REDACTED]

~~TOP SECRET//SI//NOFORN~~

 provided, however, that NSA's Office of General Counsel (OGC)



~~TOP SECRET//SI//NOFORN~~



shall first determine that any selection term reasonably believed to be used by a United States (U.S.) person is not regarded as associated with [REDACTED]  
[REDACTED]  
[REDACTED] on the basis of activities that are protected by the First Amendment to the Constitution.

(ii) Selection terms that are currently the subject of electronic surveillance authorized by the Foreign Intelligence Surveillance Court (FISC) based on the FISC's finding of probable cause to believe that they are used by [REDACTED]  
[REDACTED]  
[REDACTED] including those used by U.S. persons, may be deemed approved for querying for the period of FISC-authorized electronic surveillance without review and approval by a designated approving official. The preceding sentence shall not apply to selection terms under surveillance

[REDACTED]

pursuant to any certification of the Director of National Intelligence and the Attorney General pursuant to Section 702 of FISA, as added by the FISA Amendments Act of 2008, or pursuant to an Order of the FISC issued under Section 703 or Section 704 of FISA, as added by the FISA Amendments Act of 2008.

(iii) A determination by a designated approving official that a selection term is associated with [REDACTED] shall be effective for: one hundred eighty days for any selection term reasonably believed to be used by a U.S. person; and one year for all other selection terms.<sup>9,10</sup>

---

<sup>9</sup> The Court understands that from time to time the information available to designated approving officials will indicate that a selection term is or was associated with a Foreign Power only for a specific and limited time frame. In such cases, a designated approving official may determine that the reasonable, articulable suspicion standard is met, but the time frame for which the selection term is or was associated with a Foreign Power shall be specified. The automated query process described in the [REDACTED] Declaration limits the first hop query results to the specified time frame. Analysts conducting manual queries using that selection term shall continue to properly minimize information that may be returned within query results that fall outside of that timeframe.

[REDACTED]

(iv) Queries of the BR metadata using RAS-approved selection terms may occur either by manual analyst query or through the automated query process described below.<sup>11</sup> This automated query process queries the collected BR metadata (in a "collection store") with RAS-approved selection terms and returns the hop-limited results from those queries to a "corporate store." The corporate store may then be searched by appropriately and adequately trained personnel for valid foreign intelligence purposes, without the requirement that those searches use only RAS-approved selection terms. The specifics of the automated query process, as described in the [REDACTED] Declaration, are as follows:

[REDACTED]

<sup>11</sup> This automated query process was initially approved by this Court in its [REDACTED] 2012 Order amending docket number [REDACTED]

<sup>12</sup> As an added protection in case technical issues prevent the process from verifying that the most up-to-date list of RAS-approved selection terms is being used, this step of the automated process checks the expiration dates of RAS-approved selection terms to confirm that the approvals for those terms have not expired. This step does not use expired RAS-approved selection terms to create the list of "authorized query terms" (described below) regardless of whether the list of RAS-approved selection terms is up-to-date.

[REDACTED]

[REDACTED]

D. Results of any intelligence analysis queries of the BR metadata may be shared, prior to minimization, for intelligence analysis purposes among NSA analysts, subject to the requirement that all NSA personnel who receive query results in any form first

[REDACTED]

[REDACTED]

receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.<sup>15</sup> NSA shall apply the minimization and dissemination requirements and procedures of Section 7 of United States Signals Intelligence Directive SP0018 (USSID 18) issued on January 25, 2011, to any results from queries of the BR metadata, in any form, before the information is disseminated outside of NSA in any form. Additionally, prior to disseminating any U.S. person information outside NSA, the Director of NSA, the Deputy Director of NSA, or one of the officials listed in Section 7.3(c) of USSID 18 (*i.e.*, the Director of the Signals Intelligence Directorate (SID), the Deputy Director of the SID, the Chief of the Information Sharing Services (ISS) office, the Deputy Chief of the ISS office, and the Senior Operations Officer of the National Security Operations Center) must determine that the information identifying the U.S. person is in fact related to counterterrorism information and that it is necessary to understand the counterterrorism information or assess its importance.<sup>16</sup> Notwithstanding the above requirements, NSA may share results from intelligence analysis queries of the BR metadata, including U.S. person identifying information, with Executive Branch

---

<sup>15</sup> In addition, the Court understands that NSA may apply the full range of SIGINT analytic tradecraft to the results of intelligence analysis queries of the collected BR metadata.

<sup>16</sup> In the event the Government encounters circumstances that it believes necessitate the alteration of these dissemination procedures, it may obtain prospectively-applicable modifications to the procedures upon a determination by the Court that such modifications are appropriate under the circumstances and in light of the size and nature of this bulk collection.

personnel (1) in order to enable them to determine whether the information contains exculpatory or impeachment information or is otherwise discoverable in legal proceedings or (2) to facilitate their lawful oversight functions.

E. BR metadata shall be destroyed no later than five years (60 months) after its initial collection.

F. NSA and the National Security Division of the Department of Justice (NSD/DoJ) shall conduct oversight of NSA's activities under this authority as outlined below.

(i) NSA's OGC and Office of the Director of Compliance (ODOC) shall ensure that personnel with access to the BR metadata receive appropriate and adequate training and guidance regarding the procedures and restrictions for collection, storage, analysis, dissemination, and retention of the BR metadata and the results of queries of the BR metadata. NSA's OGC and ODOC shall further ensure that all NSA personnel who receive query results in any form first receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information. NSA shall maintain records of all such training.<sup>17</sup> OGC shall provide NSD/DoJ with copies

---

<sup>17</sup> The nature of the training that is appropriate and adequate for a particular person will depend on the person's responsibilities and the circumstances of his access to the BR metadata or the results from any queries of the metadata.

of all formal briefing and/or training materials (including all revisions thereto) used to brief/train NSA personnel concerning this authority.

(ii) NSA's ODOC shall monitor the implementation and use of the software and other controls (including user authentication services) and the logging of auditable information referenced above.

(iii) NSA's OGC shall consult with NSD/DoJ on all significant legal opinions that relate to the interpretation, scope, and/or implementation of this authority. When operationally practicable, such consultation shall occur in advance; otherwise NSD shall be notified as soon as practicable.

(iv) At least once during the authorization period, NSA's OGC, ODOC, NSD/DoJ, and any other appropriate NSA representatives shall meet for the purpose of assessing compliance with this Court's orders. Included in this meeting will be a review of NSA's monitoring and assessment to ensure that only approved metadata is being acquired. The results of this meeting shall be reduced to writing and submitted to the Court as part of any application to renew or reinstate the authority requested herein.

(v) At least once during the authorization period, NSD/DoJ shall meet with NSA's Office of the Inspector General to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders.

(vi) At least once during the authorization period, NSA's OGC and NSD/DoJ shall review a sample of the justifications for RAS approvals for selection terms used to query the BR metadata.

(vii) Prior to implementation, all proposed automated query processes shall be reviewed and approved by NSA's OGC, NSD/DoJ, and the Court.

G. Approximately every thirty days, NSA shall file with the Court a report that includes a discussion of NSA's application of the RAS standard, as well as NSA's implementation of the automated query process. In addition, should the United States seek renewal of the requested authority, NSA shall also include in its report a description of any significant changes proposed in the way in which the call detail records would be received from the Providers and any significant changes to the controls NSA has in place to receive, store, process, and disseminate the BR metadata.

Each report shall include a statement of the number of instances since the preceding report in which NSA has shared, in any form, results from queries of the BR metadata that contain United States person information, in any form, with anyone outside NSA. For each such instance in which United States person information has been shared, the report shall include NSA's attestation that one of the officials authorized to approve such disseminations determined, prior to dissemination, that the information was related to counterterrorism information and necessary to understand



counterterrorism information or to assess its importance.

This authorization regarding [REDACTED]

[REDACTED]

[REDACTED]

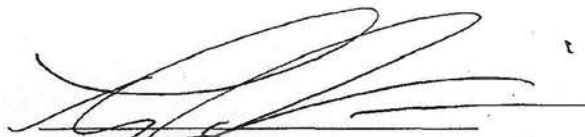
[REDACTED]

[REDACTED] expires on the 19<sup>th</sup> day

of July, 2013, at 5:00 p.m., Eastern Time.

Signed \_\_\_\_\_ Eastern Time  
                    Date           Time

04-25-2013 P02:26



ROGER VINSON  
Judge, United States Foreign  
Intelligence Surveillance Court

[REDACTED]