Questions for the Record
Senate Committee on the Judiciary Hearing on FISA
2 October 2013

QUESTIONS FOR THE RECORD – Chairman Leahy
10/2/13 FISA Hearing

Questions for NSA Director Alexander

1. During the hearing, you disagreed with the *New York Times'* characterization that the NSA has been analyzing social networks, including those of Americans, using communications metadata as well as other records. While you clarified that much of this analysis is done on foreign targets, it remains unclear how extensively the government is analyzing and chaining communications and other data involving U.S. persons.

    a. Please provide a detailed description of how this program operates and a copy of the Supplemental Procedures and Guidelines for Governing Metadata Analysis that you referenced in your testimony.
    b. Specify the types of data that are used and from whom they are obtained.
    c. Specify the particular rules that apply to the use of data involving U.S. persons and queries focused on U.S. persons.
    d. Under what legal authority or authorities is this analysis being conducted?
    e. Is the Foreign Intelligence Surveillance Court aware of this social network analysis, and has it approved the practice?
    f. What oversight is conducted of this program, and by whom?

NSA Response

a. Please provide a detailed description of how this program operates and a copy of the Supplemental Procedures and Guidelines for Governing Metadata Analysis that you referenced in your testimony.

CLASSIFIED RESPONSE OMITTED

b. Specify the types of data that are used and from whom they are obtained

NSA Response

CLASSIFIED RESPONSE OMITTED

c. Specify the particular rules that apply to the use of data involving U.S. persons and queries focused on U.S. persons.

NSA Response

The applicable rules are discussed in the answer to question 1(d) below.

d. Under what legal authority or authorities is this analysis being conducted?

NSA Response

CLASSIFIED RESPONSE OMITTED

The use and analysis of enrichment data acquired pursuant to Executive Order 12333 is also conducted pursuant to DoD Regulation 5240.1-R. Under the DoD regulation, the collection, retention, and dissemination of U.S. person information, such as that which might be included within address books and buddy lists, is subject to limitations, even if the information is publicly-available.

e. Is the Foreign Intelligence Surveillance Court aware of this social network analysis, and has it approved the practice?

NSA Response

CLASSIFIED RESPONSE OMITTED

f. What oversight is conducted of this program, and by whom?

NSA Response

Internal oversight of intelligence activities conducted pursuant to the general SIGINT authority provided in Section 1.7(c)(1) of Executive Order 12333 is performed by a number of NSA offices, to include the Office of the Inspector General and the Office of the General Counsel, as well as the Oversight and Compliance Office of the Signals Intelligence Directorate. The oversight measures include not only those pursuant to SPCMA but also the procedures outlined in the attached letter sent by NSA to the Department of Justice in 2006, when the Attorney General's approval of the procedures was requested. In addition to the terms of the letter, NSA requires analysts to identify any query known to concern a U.S. person, and such queries are subject to additional oversight to ensure that there is a valid foreign intelligence purpose for them. In addition to multiple levels of internal oversight of the SPCMA and data enrichment activities, these activities are subject to oversight by the Department of Defense IG, the Intelligence Community IG, the President's Intelligence Oversight Board and the Congress. In particular, any violation of the SPCMA procedures, like any other violation of procedures that govern NSA's handling of U.S. person information, are also covered in the quarterly intelligence oversight reports provided to the Assistant to the Secretary of Defense for Intelligence Oversight for onward reporting to the President's Intelligence Oversight Board. In addition, NSA provides an annual report to the Attorney General on (i) the kinds of information that NSA is collecting and processing as communications metadata; (ii) NSA's implementation of the SPCMA procedures; and (iii) any significant new legal or oversight issues that have arisen in connection with NSA's collection, processing or dissemination of communications metadata of U.S. persons.

2. You testified that in 2010 and 2011 the NSA received samples of "locational information" in order to test the ability of NSA systems to handle the data format. While you noted that the project ended without any actual analysis of that data, you also indicated that acquiring this type of information might be a future requirement to keep our country safe.

   a. What types of locational data did the NSA acquire in 2010 and 2011?
   b. Was the locational data of U.S. persons acquired during this test?
   c. Under what legal authority was this test conducted?
   d. What was the result of this test project?
   e. What happened to the sample location data following the conclusion of the test?
   f. How and when were the Intelligence and Judiciary Committees notified when this project was initiated?
   g. The statement released by the NSA stated that Congress would be notified if locational data were to be obtained in the future. Please confirm that the Senate and House Judiciary Committees, in particular, will be notified.

a. What types of locational data did the NSA acquire in 2010 and 2011?

NSA Response

CLASSIFIED RESPONSE OMITTED

The mobility data in the test files was kept separate from the operational dataflows. The test files were not ingested into the operational databases and were not accessible to NSA target analysts.

b. Was the locational data of U.S. persons acquired during this test?

NSA Response

CLASSIFIED RESPONSE OMITTED

c. Under what legal authority was this test conducted?

NSA Response

NSA obtained the test records pursuant to the Foreign Intelligence Surveillance Court orders in effect for the Section 215 authority at the time. NSA consulted with the Department of Justice (DoJ), which notified the Court, regarding this testing effort.

d. What was the result of this test project?

NSA Response

CLASSIFIED RESPONSE OMITTED

e. What happened to the sample location data following the conclusion of the test?

NSA Response

CLASSIFIED RESPONSE OMITTED

f. How and when were the Intelligence and Judiciary Committees notified when this project was initiated?

NSA Response

CLASSIFIED RESPONSE OMITTED

g. The statement released by the NSA stated that Congress would be notified if locational data were to be obtained in the future. Please confirm that the Senate and House Judiciary Committees, in particular, will be notified.

NSA Response

The current Primary Order requires NSA to obtain approval of the FISA Court before seeking to obtain location information in the future. As NSA has previously committed, the Senate and House Judiciary Committees would also be notified, as well as the Senate and House Intelligence Committees.

3. In Judge Bates' October 2011 FISA Court opinion, he described so-called "about" collection under Section 702 of FISA, in which communications are acquired that are not to or from a target but rather contain a reference to the name of the tasked account. Have you conducted analysis of the effectiveness of this type of collection? If so, please provide the following:

a. An explanation of the instances in which obtaining "about" communications has proven to be a uniquely valuable tool;
b. The number of terrorist plots that have been thwarted as a result of "about" collection; and
c. The number of terrorist plots with a domestic nexus that have been thwarted by the use of "about" collection.

NSA Response

NSA's authorities and capabilities work in complementary ways. The tools and methods NSA uses for tracking "use" of collected communications are based on targets and collection sources and not the specific ways in which individual communications are identified for collection from those sources. "About" communications provide unique information concerning NSA's foreign intelligence targets and provides a unique tool for target discovery and development purposes which concern analytic judgments, to include judgments about who might be involved in a terrorist plot. NSA does not specifically track the use of "about" communications and there is no reliable manner to determine how often the acquisition of such communications has played a role in thwarting a terrorist plot.

4. On October 14, the *Washington Post* reported that the NSA is harvesting hundreds of millions of contact lists and inboxes from e-mail and instant messaging accounts around the world, including many belonging to American citizens. In relation to this program, please answer the following questions:

    a. Under what legal authority is the NSA collecting these contact lists and inboxes?
    b. What legal standard are analysts required to meet in order to query or disseminate this information?
    c. When did this collection program begin and how many e-mail and instant messaging contact lists and inboxes have been acquired under this program?
    d. Please provide an estimate of the number of Americans who have had their contact lists and/or inboxes collected under this program.
    e. Please explain what the NSA does with the contact lists and inboxes once they are collected.
    f. Has the NSA ever acquired the contents of any communications under this collection program?
    g. What safeguards are in place to protect the privacy rights of Americans?
    h. Is the Foreign Intelligence Surveillance Court aware of this collection program, and has it approved such collection?
    i. What oversight is conducted of this program, and by whom?

    a. Under what legal authority is the NSA collecting these contact lists and inboxes?

NSA Response

CLASSIFIED RESPONSE OMITTED

b. What legal standard are analysts required to meet in order to query or disseminate this information?

NSA Response

CLASSIFIED RESPONSE OMITTED

c. When did this collection program begin and how many e-mail and instant messaging contact lists and inboxes have been acquired under this program?

NSA Response

CLASSIFIED RESPONSE OMITTED

d. Please provide an estimate of the number of Americans who have had their contact lists and/or inboxes collected under this program.

NSA Response

CLASSIFIED RESPONSE OMITTED

e. Please explain what the NSA does with the contact lists and inboxes once they are collected.

NSA Response

CLASSIFIED RESPONSE OMITTED

f. Has the NSA ever acquired the contents of any communications under this collection program?

NSA Response

CLASSIFIED RESPONSE OMITTED

g. What safeguards are in place to protect the privacy rights of Americans?

NSA Response

CLASSIFIED RESPONSE OMITTED

h. Is the Foreign Intelligence Surveillance Court aware of this collection program, and has it approved such collection?

NSA Response

CLASSIFIED RESPONSE OMITTED

i. What oversight is conducted of this program, and by whom?

NSA Response

CLASSIFIED RESPONSE OMITTED

October 2, 2013
Questions for the Record from Ranking Member Charles E. Grassley

General Keith Alexander, NSA Director

1. What safeguards are in place to ensure that once the telephone metadata collected under Section 215 is in the possession of the NSA, it is accessed and used only in an authorized fashion? Specifically, what safeguards help prevent (a) the searching of the metadata without the required reasonable and articulable suspicion; (b) the improper dissemination of information related to U.S. persons obtained as a result of a query of the metadata; (c) any unauthorized use whatsoever of the metadata? Under the law and current practice, to what institutions are any instances of non-compliance reported, and do these reports include the details of the non-compliance, or merely the fact that an instance of non-compliance occurred? Has anyone ever been disciplined for an instance of non-compliance? Please answer this question in an unclassified format, to the extent possible.

NSA Response

There are several internal and external safeguards in place to enable NSA's authorized use of the telephone metadata acquired under the Section 215 provision. Many of these safeguards are prescribed by the FISC's Primary Order and are also described in the attached opinions the FISC issued concerning the program on 29 August 2013 and 11 October 2013.

NSA employs a selector management tool that houses all Reasonable Articulable Suspicion (RAS)-approved selectors and their required nomination justification. The system also provides for the enforcement of the approval process, required by the FISC Order, that all RAS nominations are approved by one of the twenty-two officials named in accordance with the Order and that any nominated selector known to be used by a U.S. person is reviewed and approved by NSA's Office of General Counsel to ensure that the justification was not solely based on activities that are protected by the First Amendment to the Constitution.

Access controls prohibit query access by personnel who have not been appropriately and adequately trained or who do not have the proper credentials authorizing them to conduct queries of the acquired telephony metadata. NSA employs technical safeguards that allow only authorized personnel to query the BR metadata repository, for intelligence analysis purposes, using only selectors on the RAS-approved list (prohibiting queries of non-RAS approved selectors), and that allow queries to be conducted only out to the authorized three hops (again, prohibiting queries from continuing beyond the authorized third hop). These queries are then audited to assess their compliance with the Court's requirements. NSA audits these queries every 30 days.

The telephone metadata is subject to a 5-year retention limitation pursuant to the FISC Order.

In accordance with the FISC Order, NSA and DoJ meet quarterly for the purpose of assessing NSA's compliance with the Court's orders. DOJ audits all U.S. person RAS determinations from the previous quarter and a sampling of non-US. person RAS determinations from the previous quarter.

To safeguard against improper dissemination of information related to U.S persons obtained as a result of a query into the metadata, NSA relies on management controls, the training regimen required of the analyst to include an enhanced training course specifically on the requirements of handling data under this authority, and internal NSA policy. As it relates to this authority, prior to disseminating any U.S. person information outside NSA, an official holding one of the seven positions named within the Order 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.

In accordance with the FISC Order, approximately every thirty days, NSA files with the Court a report that includes a discussion of NSA's application of the RAS standard and the number of instances since the preceding report in which NSA has shared, in any form, results from the queries of the telephony metadata, that contain U.S. person information, in any form, with anyone outside the NSA and includes an attestation that one of the officials authorized to approve such disseminations determined that the information was related to counterterrorism information and necessary to understand counterterrorism information or to assess its importance.

All RAS determinations are documented. Intelligence analysis queries are audited, analysts are trained on the use of the data, and all BR metadata is tagged and only accessible by personnel with appropriate credentials. Here again, NSA relies heavily upon management controls, the training regimen required by NSA employees that includes enhanced training on the requirements of handling data under this authority, as well as internal NSA policy.

Executive Branch oversight of the BR FISA program includes the following practices for reporting instances of non-compliance and conducting oversight of the program:

- NSA reports instances of noncompliance to DoJ and ODNI. These reports include details about the non-compliance.
- DoJ and ODNI meet with NSA at least once during the authorization period (typically 90 days) to review NSA's processes and its assessment that only approved metadata is being acquired.
- NSA's Inspector General and Office of the Director of Compliance are assigned specific BR FISA oversight responsibilities by the Court.
- NSA consults with DoJ on all significant legal interpretations of the BR FISA authority.
- As noted above, DoJ reviews a sample of the selection terms approved to query the telephony metadata.

- NSA also provides an Intelligence Oversight Quarterly Report to the President's Intelligence Oversight Board through the Assistant to the Secretary of Defense for Intelligence Oversight. This report, which includes details about noncompliance incidents, is produced by the NSA Office of the Inspector General and the NSA Office of General Counsel, and signed by the NSA Inspector General, the NSA General Counsel, and NSA Director.

Judicial Branch oversight includes:

- The Foreign Intelligence Surveillance Court Rules of Procedure require the Government to report to the Court in writing any non-compliance with the Court's approvals or authorizations, including incidents of noncompliance with Court-approved minimization procedures or applicable law. The Government must include a description of the facts and circumstances of the non-compliance, any modifications the Government has made or proposes to make in its implementation of the affected authority, and how the Government intends to dispose of or treat any information obtained as a result of the non-compliance.
- NSA also provides regular 30 day reports to the FISC that describe its application of the RAS standard, its implementation, and the operation of an authorized automated query process (described below), and the number of disseminations of query results that contain U.S. person information made during the reporting period.
- NSA reports upon renewal any significant changes in the way NSA receives call detail records or changes to NSA's controls to receive, store, process, and disseminate BR metadata.
- The FISC must renew the authorization the BR FISA program every 90 days.

Legislative oversight includes:

- The National Security Act and FISA impose requirements to report certain incidents of noncompliance to the designated congressional oversight committees. These reports include details about the compliance incidents, and at a committee's request, NSA will provide detailed classified briefing(s) regarding the incident.
- ODNI and NSA also provide extensive briefings to the Congressional intelligence and judiciary committees on NSA's operation of the BR FISA bulk telephony metadata program.
- ODNI and NSA also provide Congress with written notifications regarding all significant developments in the program.
- The Department of Justice provides Congress with copies of all significant FISC opinions regarding the BR FISA program.

In addition, the BR FISA statutory provision requires the Attorney General, on an annual basis, to report to the intelligence and judiciary committees of the Congress (50 U.S.C. 1862):

- The total number of BR FISA applications;
- The total number of BR FISA orders either granted, modified, or denied; and

- The total number of orders either granted, modified, or denied that concerned library circulation records, firearms sales records, tax return records, educational records, or medical records that would identify a person.

NSA takes appropriate remedial action with respect to any compliance incident. NSA personnel may be subject to disciplinary action in connection with compliance matters whenever appropriate. There have been no identified instances of willful noncompliance in connection with the BR FISA program.

Hearing: "Continued Oversight of the Foreign Intelligence Surveillance Act"
Sen. Sheldon Whitehouse
Questions for the Record

Questions for The Honorable Keith B. Alexander, Director, National Security Agency

1. The sudden, unauthorized disclosure of classified information by Edward Snowden appeared to catch the intelligence community without a protocol for responding to such an eventuality. How have you revised your procedures since the Snowden incident to respond more effectively to sudden, unauthorized disclosures of classified information?

   Response

   An interagency response will be provided under separate cover.

2. As the Snowden incident revealed, the Intelligence Community relies heavily on private contractors for a variety of functions. What ensures that the government's reliance on contractors is not so great that appropriate legal redress cannot be taken against contractors in cases of misconduct, and that defense and intelligence contractors are not, in effect, "too big to sue"?

   Response

   An interagency response will be provided under separate cover.

3. While the bulk telephony metadata collection program under Section 215 of the USA PATRIOT Act appears to be legal and constitutional, the program is potentially susceptible to abuse. Robust oversight is critical to preventing and addressing such abuse. Please list all of the executive, legislative, and judicial oversight that reviews the program.

   Response

   An interagency response will be provided under separate cover.

   NSA Response

There are several internal and external safeguards in place to enable NSA's authorized use of the telephone metadata acquired under the Section 215 provision. Many of these safeguards are prescribed by the FISC's Primary Order and are also described in the attached opinions the FISC issued concerning the program on 29 August 2013 and 11 October 2013.

NSA employs a selector management tool that houses all Reasonable Articulable Suspicion (RAS)-approved selectors and their required nomination justification. The system also provides for the enforcement of the approval process, required by the FISC Order, that all RAS

nominations are approved by one of the twenty-two officials named in accordance with the Order and that any nominated selector known to be used by a U.S. person is reviewed and approved by NSA's Office of General Counsel to ensure that the justification was not solely based on activities that are protected by the First Amendment to the Constitution.

Access controls prohibit query access by personnel who have not been appropriately and adequately trained or who do not have the proper credentials authorizing them to conduct queries of the acquired telephony metadata. NSA employs technical safeguards that allow only authorized personnel to query the BR metadata repository, for intelligence analysis purposes, using only selectors on the RAS-approved list (prohibiting queries of non-RAS approved selectors), and that allow queries to be conducted only out to the authorized three hops (again, prohibiting queries from continuing beyond the authorized third hop). These queries are then audited to assess their compliance with the Court's requirements. NSA audits these queries every 30 days.

The telephone metadata is housed in a segregated database and the metadata is subject to a 5-year retention limitation pursuant to the FISC Order.

In accordance with the FISC Order, NSA and DoJ meet quarterly for the purpose of assessing NSA's compliance with the Court's orders. DOJ audits all U.S. person RAS determinations from the previous quarter and a sampling of non-US. person RAS determinations from the previous quarter.

To safeguard against improper dissemination of information related to U.S persons obtained as a result of a query into the metadata, NSA relies on management controls, the training regimen required of the analyst to include an enhanced training course specifically on the requirements of handling data under this authority, and internal NSA policy. As it relates to this authority, prior to disseminating any U.S. person information outside NSA, an official holding one of the seven positions named within the Order 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.

In accordance with the FISC Order, approximately every thirty days, NSA files with the Court a report that includes a discussion of NSA's application of the RAS standard and the number of instances since the preceding report in which NSA has shared, in any form, results from the queries of the telephony metadata, that contain U.S. person information, in any form, with anyone outside the NSA and includes an attestation that one of the officials authorized to approve such disseminations determined that the information was related to counterterrorism information and necessary to understand counterterrorism information or to assess its importance.

All RAS determinations are documented. Intelligence analysis queries are audited, analysts are trained on the use of the data, and all BR metadata is tagged and only accessible by personnel with appropriate credentials. Here again, NSA relies heavily upon management controls, the training regimen required by NSA employees that includes enhanced training on the requirements of handling data under this authority, as well as internal NSA policy.

Executive Branch oversight of the BR FISA program includes the following practices for reporting instances of non-compliance and conducting oversight of the program:

- NSA reports instances of noncompliance to DoJ and ODNI. These reports include details about the non-compliance.
- DoJ and ODNI meet with NSA at least once during the authorization period (typically 90 days) to review NSA's processes and its assessment that only approved metadata is being acquired.
- NSA's Inspector General and Office of the Director of Compliance are assigned specific BR FISA oversight responsibilities by the Court.
- NSA consults with DoJ on all significant legal interpretations of the BR FISA authority.
- As noted above, DoJ reviews a sample of the selection terms approved to query the telephony metadata.
- NSA also provides an Intelligence Oversight Quarterly Report to the President's Intelligence Oversight Board through the Assistant to the Secretary of Defense for Intelligence Oversight. This report, which includes details about noncompliance incidents, is produced by the NSA Office of the Inspector General and the NSA Office of General Counsel, and signed by the NSA Inspector General, the NSA General Counsel, and NSA Director.

Judicial Branch oversight includes:

- The Foreign Intelligence Surveillance Court Rules of Procedure require the Government to report to the Court in writing any non-compliance with the Court's approvals or authorizations, including incidents of noncompliance with Court-approved minimization procedures or applicable law. The Government must include a description of the facts and circumstances of the non-compliance, any modifications the Government has made or proposes to make in its implementation of the affected authority, and how the Government intends to dispose of or treat any information obtained as a result of the non-compliance.
- NSA also provides regular 30 day reports to the FISC that describe its application of the RAS standard, its implementation, and the operation of an authorized automated query process (described below), and the number of disseminations of query results that contain U.S. person information made during the reporting period.
- NSA reports upon renewal any significant changes in the way NSA receives call detail records or changes to NSA's controls to receive, store, process, and disseminate BR metadata.
- The FISC must reauthorize the BR FISA program every 90 days.

Legislative oversight includes:

- The National Security Act and FISA impose requirements to report certain incidents of noncompliance to the designated congressional oversight committees. These

reports include details about the compliance incidents, and at a committee's request, NSA will provide detailed classified briefing(s) regarding the incident.

- ODNI and NSA also provide extensive briefings to the Congressional intelligence and judiciary committees on NSA's operation of the BR FISA bulk telephony metadata program.
- ODNI and NSA also provide Congress with written notifications regarding all significant developments in the program.
- The Department of Justice provides Congress with copies of all significant FISC opinions regarding the BR FISA program.

In addition, the BR FISA statutory provision requires the Attorney General, on an annual basis, to report to the intelligence and judiciary committees of the Congress (50 U.S.C. 1862):

- The total number of BR FISA applications;
- The total number of BR FISA orders either granted, modified, or denied; and
- The total number of orders either granted, modified, or denied that concerned library circulation records, firearms sales records, tax return records, educational records, or medical records that would identify a person.

NSA takes appropriate remedial action with respect to any compliance incident. NSA personnel may be subject to disciplinary action in connection with compliance matters whenever appropriate. There have been no identified instances of willful noncompliance in connection with the BR FISA program.

4. Please provide an unclassified, simple summary of the mitigation procedures that govern the bulk telephony metadata collection program.

NSA Response

Query Terms: Under the FISC orders authorizing the collection, authorized analytic queries may begin only with selection term that is associated with one of the FISC-approved foreign terrorist organizations. An identifier used to commence a query of the data is referred to as a "seed." Specifically, under Court-approved rules applicable to the program, there must be a "reasonable, articulable suspicion" that a seed identifier used to query the data for foreign intelligence purposes is associated with a particular foreign terrorist organization. No more than twenty-two designated NSA officials can make a finding that there is "reasonable, articulable suspicion" that a seed identifier proposed for query is associated with a specific foreign terrorist organization. Further, when the seed identifier is reasonably believed to be used by a U.S. person, the suspicion of an association with a particular foreign terrorist organization cannot be based solely on activities protected by the First Amendment. NSA's Office of the General Counsel must review and approve any such findings for selection terms believed to be used by U.S. persons.

Query results: Raw results of authorized queries are available only to those analysts trained in the restrictions on the handling and dissemination of the metadata. Query results can be further analyzed only for valid foreign intelligence purposes.

Retention: The raw metadata collected as part of this program is destroyed no later than five years (60 months) after its initial collection.

Dissemination: NSA may disseminate any results from queries of the metadata subject to its generally applicable dissemination requirements governing its E.O. 12333 collection. Additionally, prior to disseminating any U.S. person information outside NSA, one of seven specified NSA officials 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. More detailed descriptions of the Court-ordered minimization procedures applicable to this program may be found in the recently declassified and published Primary Orders issued by the FISC. See http://www.dni.gov/files/documents/PrimaryOrder_Collection_215.pdf.

5. Has the Foreign Intelligence Surveillance Court's review of the bulk telephony metadata program yet considered the Supreme Court case *United States v. Jones*, 132 S. Ct. 945 (2012), and particularly Justice Sotomayor's concurring opinion in *Jones*? Please share any relevant analysis by the FISC in an unclassified format.

NSA Response

On 11 October 2013, Judge McLaughlin of the FISC issued a Memorandum Opinion, which has been declassified and published by the FISC, explaining her decision to grant the Government's Application renewing the program. Judge McLaughlin addressed the *Jones* decision on pages 4–6 of the Memorandum Opinion. A copy of the Memorandum Opinion is attached and also is available at http://www.uscourts.gov/uscourts/courts/fisc/br13-158-memo-131018.pdf.

QUESTIONS FOR THE RECORD
Senate Judiciary Committee
"Continued Oversight of the Foreign Intelligence Surveillance Act"
October 2, 2013
Senator Amy Klobuchar

Questions for General Keith B. Alexander

As discussed at the hearing, in mid-August 2013, the media began reporting about an internal audit from May 2012, which found that the NSA violated privacy rules numerous times. This audit was not brought to the Senate Judiciary Committee's attention at the July 31, 2013 hearing on FISA surveillance programs.

- Can you describe how the results of internal audits or investigations of the Intelligence Community, and the NSA in particular, are communicated to Congress or the public?

NSA Response

NSA conducts a number of internal audits, inspections, compliance reviews, and incident reporting, both as part of its internal oversight and compliance programs and to support specific external reporting requirements, as mandated by law and policy.

The referenced document, "NSAW SID Intelligence Oversight (IO) Quarterly Report – First Quarter Calendar Year 2012 (1 January-31 March 2012 – EXECUTIVE SUMMARY, is used internally at NSA to improve its oversight and compliance programs. Information contained in the document (and other internal NSA documents regarding oversight and compliance) forms the basis of a number of submissions to Congress, including but not limited to:

1. Semi-Annual Report to Congress – As required by Section 5 of the IG Act of 1978 (as amended), the NSA Office of the Inspector General (OIG) prepares and sends a *Semi-annual Report to Congress*, which includes descriptions of reports produced by the OIG during the reporting period and significant outstanding recommendations from previous reports. The report is furnished to the Director of NSA, who provides the report, along with his own statutorily required report, to the Chairman and Vice Chairman of the SSCI and to the Chairman and Ranking Member of the HPSCI.

2. Annual FAA §702 Report – The NSA OIG prepares an annual report to Congress on compliance with the targeting and minimization procedures of Section 702 of the Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (FAA §702).

- The report is due to Congress by 31 December of each year. It has been prepared and submitted yearly since the FY 2009 report. This report is provided to the Chairman (and Vice Chairman where applicable) and Ranking Members of the House and Senate Intelligence and Judiciary Committees.

3. Other – NSA's Office of the Inspector General responds to Committee requests for information, most recently by a letter date 11 September 2013 to Chairman Leahy and Ranking Member Grassley.

- Will you consider disseminating the results of internal audits or investigations more widely to Congress and the public in order to help improve the transparency of Intelligence Community activities linked to bulk collection?

NSA Response

NSA, along with ODNI and DoJ, will continue our efforts to promote greater transparency while carefully protecting information that we cannot responsibly release because of national security concerns, and we will work with the Intelligence and Judiciary Committees if additional information is required beyond what is already being furnished.

Senator Mazie K. Hirono

Questions for the Record following hearing on October 2, 2013 entitled:
"Continued Oversight of the Foreign Intelligence Surveillance Act"

The Honorable Keith B. Alexander, Director, National Security Agency

1. At the hearing I asked if the Intelligence Community and the NSA specifically are focusing on evolving the technology of privacy safeguards as the surveillance technology is clearly evolving.

    a. Can you give examples of what kinds of new technical capacity to protect privacy we can expect to benefit from in the future?
    b. Is the NSA working to develop narrower, more targeted collection or is all the research and development focused on expanding access to information?
    c. Can you give examples of what kinds of new technical capacity to protect privacy we can expect to benefit from in the future?

NSA Response

CLASSIFIED RESPONSE OMITTED

NSA's internal compliance program, spearheaded by the Office of the Director of Compliance (ODOC), includes formation of a novel rules architecture designed to accurately reflect the complete set of rules protecting privacy. This rules architecture is an essential component of NSA's Smart Data initiatives, as it enables systems to apply critical data tags that discern the specific authorization under which NSA collected or acquired specific data. That information informs access controls which prevent an individual from seeing data for which they have not been trained and/or do not have a mission need.

ODOC developed and manages Verification of Accuracy procedures to provide an increased level of confidence that factual representations are based on an ongoing shared understanding among operational, technical, legal, policy, and compliance officials. NSA has applied them to authority-related documentation, especially when describing complex technical matters to NSA's overseers.

NSA also leverages a number of technology solutions to ultimately assist and audit analysts as they perform their job. For example, NSA uses an access control architecture that prevents personnel from accessing collected data unless they have the required credentials and training. NSA also uses appropriate mission sponsorship and an accountability system that provides a repository of queries to NSA data and the ability to perform post-query auditing. NSA continues to explore new ways to develop and enhance its use of technology to support and enforce privacy protections for its SIGINT and other mission data.

2. Is the NSA working to develop narrower, more targeted collection or is all the research and development focused on expanding access to information?

NSA Response

CLASSIFIED RESPONSE OMITTED

3. It has been reported that certain data collected by the NSA are shared with domestic law enforcement agencies.

    a. What is the legal authority that allows the NSA to give Section 215 of the Patriot Act and FISA Amendments Act Section 702 data to other agencies such as the FBI, DEA, or other law enforcement agencies?
    b. Does such sharing require the demonstration of "probable cause" before such data are shared?
    c. Is the FISA court involved in such approvals on a case-by-case basis?
    d. What is the legal authority that allows the NSA to give Section 215 of the Patriot Act and FISA Amendments Act Section 702 data to other agencies such as the FBI, DEA, or other law enforcement agencies?

NSA Response

NSA disseminates foreign intelligence information derived from both lawful queries of Section 215 data and FAA Section 702 targeting to intelligence components of law enforcement agencies, including the intelligence components of the FBI, in response to approved foreign intelligence requirements. The Foreign Intelligence Surveillance Act also requires minimization procedures to include "procedures that allow for the retention and dissemination of information that is evidence of a crime . . . and that is to be retained or disseminated for law enforcement purposes (section 101 of the FISA). Section 106 of the FISA also sets forth specific requirements that are applicable to law enforcement use of certain types of FISA collection.

Section 215

The legal authority that allows NSA to disseminate information derived from lawful queries of Section 215 data is found within the applicable orders of the FISC. The FISC's Primary Order permits NSA to disseminate any results from queries of the Section 215 metadata subject to the minimization and dissemination requirements and procedures of United States Signals Intelligence Directive SP0018 (USSID 18). The Primary Order also requires that, prior to disseminating any U.S. person information outside NSA, one of seven specified NSA officials 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. Certain disseminations are not subject to the foregoing requirement. The Primary Order states that "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 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."

NSA disseminates information derived from queries of Section 215 data for counterterrorism intelligence purposes, not law enforcement purposes. Apart from the FBI, which has a counterterrorism intelligence mission, NSA does not as a matter of practice disseminate Section 215 results directly to any agencies with a law enforcement mission, including the DEA.

FAA Section 702

FAA Section 702 provides for the targeting of non-U.S. persons reasonably believed to be located outside the United States to acquire foreign intelligence information. NSA processes FAA Section 702 acquired data in accordance with FISA Court-reviewed minimization procedures and disseminates foreign intelligence information in accordance with the standards set forth in those procedures to recipients who require the information in the performance of official duties.

The legal authority that allows NSA to disseminate information derived from FAA Section 702 targeting is found within the minimization procedures adopted by the Attorney General, in consultation with the Director of National Intelligence, and approved by the FISA Court. See 50 U.S.C. § 1881a(e). These procedures authorize NSA to disseminate 702-acquired information not concerning any U.S. persons in accordance with other applicable law, regulation and policy. The procedures impose stringent requirements for the dissemination of communications of or concerning a U.S. person; such communications may be disseminated only if certain conditions are satisfied (e.g., a report containing the identity of a U.S. person may be disseminated if the identity is necessary to understand foreign intelligence information or assess its importance.) Foreign intelligence includes information concerning international terrorist activities, and other hostile activities directed against the U.S. by foreign powers, entities, persons and their agents. While there are numerous foreign intelligence topics which are of interest both to the foreign intelligence and law enforcement communities, NSA's core mission is to disseminate information for the purpose of advancing national security interests not criminal prosecutions. The Attorney General-adopted and FISA Court-approved minimization procedures applicable to NSA's FAA Section 702 collection separately authorize the retention and dissemination to appropriate law enforcement authorities of information that is reasonably believed to contain evidence of a crime.

Other authorities separately require NSA to report to DoJ information relating to potential crimes. For example, Section 1.7(a) of Executive Order 12333 requires NSA to "report to the Attorney General possible violations of the federal criminal laws by employees and of specified federal criminal laws by any other person . . . as specified in [agreed upon] procedures."

a. Does such sharing require the demonstration of "probable cause" before such data are shared?

NSA Response

NSA does not need to demonstrate "probable cause" prior to disseminating the results of either a lawful Section 215 query or FAA Section 702 targeting, but rather must comply with the requirements listed above in the answer to Question 2(a). Any recipient agency may use the disseminated information as permitted by its own legal authorities.

b. Is the FISA court involved in such approvals on a case-by-case basis?

NSA Response

Section 215

The FISA Court does not approve disseminations of Section 215 data on a case-by-case basis. The FISA Court receives a monthly report from NSA that includes a list of all disseminations, in any form, of U.S. person information that occurred within the period covered by the report. This list includes the date of the dissemination, the recipient(s) of the dissemination, and the form of the dissemination (e.g., formal intelligence report, e-mail, verbal communication).

FAA Section 702

The FISA Court does not approve disseminations of FAA Section 702 data on a case-by-case basis. All disseminations of FAA section 702 data are available for review by DoJ and ODNI, whose representatives conduct oversight of NSA's exercise of the authority under FAA section 702 approximately once every 60 days. DoJ and ODNI review disseminations to ensure that NSA complies with the applicable minimization procedures, including any disseminations regarding criminal activity.

4. At the hearing I asked if PRISM is the only intelligence program NSA runs under FISA Section 702 and what other programs are run under sections 215 and 702.

   a. Please provide a complete list of the programs and their purposes that are operated by the NSA under the authorities provided by sections 215 and 702?

NSA Response

CLASSIFIED RESPONSE OMITTED

5. In conducting the programs under Sections 215 and 702 authorities, could less intrusive methods of collection have yielded the same information?

NSA Response

CLASSIFIED RESPONSE OMITTED

6. At the hearing several questions were asked related to the recent disclosure by the NSA Inspector General that 12 instances of intentional misuse of signals intelligence authorities of the Director of the National Security Agency.

    a. You indicated that "highlighting the punishments that go along with this" type of misuse should help prevent future instances of this type of misuse. Do you believe that increased criminal penalties for this type of privacy violation by intelligence analysts would help with deterrence?

NSA Response

It is difficult to predict whether increased criminal penalties for intentional violations of SIGINT authorities would help to deter the kinds of misuse reported by NSA's Inspector General. The small number of reported incidents suggests that existing remedies may be sufficient to deter unlawful conduct for the vast majority of the workforce.