	DATE OF DOCUMENT	TITLE OF DOCUMENT	DESCRIPTION
(1)	06/05/2013	Statements By Edward Snowden Publicly Disclosing the Government Surveillance	Statements by NSA whistleblower, Edward Snowden, disclosing the NSA surveillance.
(2)	04/25/2013	Section 215- Secondary Order ("Verizon Order")	A Foreign Intelligence Surveillance Court ("FISC") order approving the application of Section 215 for Verizon metadata collection
(3)	10/11/2013	FISC Primary Order and Memorandum	FISC memorandum and primary order granting the government's request for ongoing daily production to the NSA of "certain telephone call detail records in bulk"
(4)	4/13/2013	PRISM PowerPoint Slides Re: Data Acquisition	NSA training slides about the acquisition of surveillance information through the PRISM program.
(5)	03/14/2013	NSA: Special Operations Weekly Excerpt	An excerpt from the Special Operations Weekly-an internal NSA publication describing data collection via the MUSCULAR program .
(6)	02/25/2009	NSA Memo: Congressional Notification and Incidents of Compliance	An NSA memo to notify the House Permanent Selection Committee on Intelligence compliance Incidents identified under the ongoing end-to-end review of bulk telephony metadata under Section 215.
(7)	05/03/2012	SID Oversight and Compliance	A 2012 quarterly audit of the NSA's surveillance activities, which describes 2,766 violations by the NSA of the surveillance laws and its internal rules and regulations.
(8)	08/28/2013	Grassley Presses For Details About Intentional Abuse of NSA Authorities	Senator Chuck Grassley's letter to Dr. George Ellard, Inspector General of the National Security Agency.

(9)	09/11/2013	Dr. Ellard letter to Senator Grassley	Letter in Response to Senator Chuck Grassley by Dr. George Ellard, Inspector General of the National Security Agency.
(10)	06/21/ 2013	Director Clapper letter to Senator Feinstein	Letter from the Director of National Intelligence, James Clapper, to Senator Dianne Feinstein, Chairman of the Select Committee on Intelligence.
(11)	06/24/2013	Wyden-Udall Letter on NSA Fact Sheet Inaccuracy	A letter from Senators Wyden and Udall to General Alexander on a "significant" inaccuracy in the NSA's Section 702 fact sheet.
(12)	06/25/2013	General Alexander Letter Re: NSA Fact Sheet Inaccuracy	A letter from General Alexander responding to Senators Wyden and Udall about the NSA's Section 702 fact sheet inaccuracy.
(13)	06/18/2013	NSA Section 702 and Section 215 Fact Sheets	NSA factsheets on Section 702 of FISA and Section 215 of the Patriot Act that were later withdrawn after Senators Wyden and Udall complained of Section 702 inaccuracies.
(14)	09/06/2013	Congressman Sensenbrenner letter to Attorney General Holder	Congressman Sensenbrenner letter to Attorney General Holder questioning the interpretation of Section 215 of the Patriot Act.
(15)	03/15/2013	Senators Wyden and Udall letter to Attorney General Holder	Senators Wyden and Udall letter to Attorney General Holder questioning the interpretation of Section 15 of the Patriot Act.
(16)	10/12/2011	FAA Certification Renewals with Caveats	An NSA document describing the FISA Court's 2011 FAA Certifications and noting the FISC ruling that certain procedures for the collection of "Multiple Communications Transactions" were "deficient on statutory and constitutional grounds."
(17)	07/02/2013	Letter from the ACLU to the Honorable William H. Pauley III	Pre-motion letter sent by the ACLU to the Honorable William H. Pauley III.

(18)	07/29/2013	Response of the Honorable Reggie B. Walton to Chairman Patrick K. Leahy of the Committee on the Judiciary	Response of the Honorable Reggie B. Walton to Chairman Patrick K. Leahy of the Committee on the Judiciary
(19)	03/26/2009	Declaration of Mark Klein (former employee of AT&T)	Declaration of Mark Klein submitted by the Electronic Frontier Foundation in support of preliminary injunction, discussing the NSA's involvement with AT&T.
(20)	10/03/2011	FISC Memorandum Opinion- October 2011 (Judge Bates)	A FISC opinion ruling one electronic communications collection program unconstitutional
(21)	11/13/2013	Notice to Appear at Oral Argument and *Touhy* request	Notice to Appear at Oral Argument and *Touhy* request sent to the NSA Defendant on November 13, 2013 by the Plaintiffs.

Exhibit 1

Edward Snowden Interview Transcript FULL TEXT: Read the Guardian's Entire Interview With the Man Who Leaked PRISM
Image Credit: The Guardian

The NSA whistleblower who revealed the PRISM program has publically revealed himself to be Edward Snowdern, a former private contactor for the NSA. He gave an interview with journalist Glenn Greenwald about his thoughts on his reasons behind whistleblowing and what what his experience in the NSA was like. The following is a transcript of the entire video interview.

Edward Snowden: "My name is Ed Snowden, I'm 29 years old. I worked for Booz Allen Hamilton as an infrastructure analyst for NSA in Hawaii.

Glenn Greenwald: "What are some of the positions that you held previously within the intelligence community?"

Snowden: "I've been a systems engineer, systems administrator, senior adviser for the Central Intelligence Agency, solutions consultant, and a telecommunications informations system officer."

Greenwald: "One of the things people are going to be most interested in, in trying to understand what, who you are and what you are thinking is there came some point in time when you crossed this line of thinking about being a whistleblower to making the choice to actually become a whistleblower. Walk people through that decision making process."

Snowden: "When you're in positions of privileged access like a systems administrator for the sort of intelligence community agencies, you're exposed to a lot more information on a broader scale then the average employee and because of that you see things that may be disturbing but over the course of a normal person's career you'd only see one or two of these instances. When you see everything you see them on a more frequent basis and you recognize that some of these things are actually abuses. And when you talk to people about them in a place like this where this is the normal state of business people tend not to take them very seriously and move on from them."

"But over time that awareness of wrongdoing sort of builds up and you feel compelled to talk about. And the more you talk about the more you're ignored. The more you're told its not a problem until eventually you realize that these things need to be determined by the public and not by somebody who was simply hired by the government."

Greenwald: "Talk a little bit about how the American surveillance state actually functions. Does it target the actions of Americans?"

Snowden: "NSA and intelligence community in general is focused on getting intelligence wherever it can by any means possible. It believes, on the grounds of sort of a self-certification, that they serve the national interest. Originally we saw that focus very narrowly tailored as foreign intelligence gathered overseas."

"Now increasingly we see that it's happening domestically and to do that they, the NSA specifically, targets the communications of everyone. It ingests them by default. It collects them in its system and it filters them and it analyses them and it measures them and it stores them for periods of time simply because that's the easiest, most efficient, and most valuable way to achieve these ends. So while they may be intending to target someone associated with a foreign government or someone they suspect of terrorism, they're collecting you're communications to do so."

"Any analyst at any time can target anyone, any selector, anywhere. Where those communications will be picked up depends on the range of the sensor networks and the authorities that analyst is empowered with. Not all analysts have the ability to target everything. But I sitting at my desk certainly had the authorities to wiretap anyone from you or your accountant to a Federal judge to even the President if I had a personal e-mail."

Greenwald: "One of the extraordinary parts about this episode is usually whistleblowers do what they do anonymously and take steps to remain anonymous for as long as they can, which they hope often is forever. You on the other hand have decided to do the opposite, which is to declare yourself openly as the person behind these disclosures. Why did you choose to do that?"

Snowden: "I think that the public is owed an explanation of the motivations behind the people who make these disclosures that are outside of the democratic model. When you are subverting the power of government that's a fundamentally dangerous thing to democracy and if you do that in secret consistently as the government does when it wants to benefit from a secret action that it took. It'll kind of give its officials a mandate to go, 'Hey tell the press about this thing and that thing so the public is on our side.' But they rarely, if ever, do that when an abuse occurs. That falls to individual citizens but they're typically maligned. It becomes a thing of 'These people are against the country. They're against the government' but I'm not."

"I'm no different from anybody else. I don't have special skills. I'm just another guy who sits there day to day in the office, watches what's happening and goes, 'This is something that's not our place to decide, the public needs to decide whether these programs and policies are right or wrong.' And I'm willing to go on the record to defend the authenticity of them and say, 'I didn't change these, I didn't modify the story. This is the truth; this is what's happening. You should decide whether we need to be doing this.'"

Greenwald: "Have you given thought to what it is that the US government's response to your conduct is in terms of what they might say about you, how they might try to depict you, what they might try to do to you?"

Snowden: "Yeah, I could be rendered by the CIA. I could have people come after me. Or any of the third-party partners. They work closely with a number of other nations. Or they could pay off the Traids. Any of their agents or assets. We've got a CIA station just up the road and the consulate here in Hong Kong and I'm sure they're going to be very busy for the next week. And that's a fear I'll live under for the rest of my life, however long that happens to be."

"You can't come forward against the world's most powerful intelligence agencies and be completely free from risk because they're such powerful adversaries. No one can meaningfully oppose them. If they want to get you, they'll get you in time. But at the same time you have to make a determination about what it is that's important to you. And if living unfreely but comfortably is something you're willing to accept, and I think it many of us are it's the human nature; you can get up everyday, go to work, you can collect your large paycheck for relatively little work against the public interest, and go to sleep at night after watching your shows."

"But if you realize that that's the world you helped create and it's gonna get worse with the next generation and the next generation who extend the capabilities of this sort of architecture of oppression, you realize that you might be willing to accept any risk and it doesn't matter what the outcome is so long as the public gets to make their own decisions about how that's applied."

Greenwald: "Why should people care about surveillance?"

Snowden: "Because even if you're not doing anything wrong you're being watched and recorded. And the storage capability of these systems increases every year consistently by orders of magnitude to where it's getting to the point where you don't have to have done anything wrong. You simply have to eventually fall under suspicion from somebody even by a wrong call. And then they can use this system to go back in time and scrutinize every decision you've ever made, every friend you've ever discussed something with. And attack you on that basis to sort to derive suspicion from an innocent life and paint anyone in the context of a wrongdoer."

Greenwald: "We are currently sitting in a room in Hong Kong, which is where we are because you travelled here. Talk a little bit about why it is that you came here and specifically there are going to be people…people speculate that what you really intend to do is to defect to the country that many see as the number one rival of the Untied States, which is China. And that what you are really doing is essentially seeking to aid an enemy of the United States with which you intend to seek asylum. Can you talk a little about that?"

Snowden: "Sure. So there's a couple assertions in those arguments that are sort of embedded in the questioning of the choice of Hong Kong. The first is that China is an enemy of the United States. It's not. I mean there are conflicts between the United States government and the Chinese PRC government but the peoples inherently we don't care. We trade with each other freely, we're not at war, we're not in armed conflict, and we're not trying to be. We're the largest trading partners out there for each other."

"Additionally, Hong Kong has a strong tradition of free speech. People think 'Oh China, Great Firewall.' Mainland China does have significant restrictions on free speech but the people of Hong Kong have a long tradition of protesting in the streets, of making there views known. The internet is not filtered here more so then any other western government and I believe that the Hong Kong government is actually independent in relation to a lot of other leading western governments."

Greenwald: "If your motive had been to harm the United States and help its enemies or if your motive had been personal material gain were there things you could have done with these documents to advance those goals that you didn't end up doing?"

Snowden: "Oh absolutely. Anyone in the positions of access with the technical capabilities that I had could suck out secrets, pass them on the open market to Russia; they always have an open door as we do. I had access to the full rosters of everyone working at the NSA, the entire intelligence community, and undercover assets all over the world. The locations of every station, we have what their missions are and so forth."

"If I had just wanted to harm the US? You could shut down the surveillance system in an afternoon. But that's not my intention. I think for anyone making that argument they need to think, if they were in my position and you live a privileged life, you're living in Hawaii, in paradise, and making a ton of money, 'What would it take you to leave everything behind?'"

"The greatest fear that I have regarding the outcome for America of these disclosures is that nothing will change. People will see in the media all of these disclosures. They'll know the lengths that the government is going to grant themselves powers unilaterally to create greater control over American society and global society. But they won't be willing to take the risks necessary to stand up and fight to change things to force their representatives to actually take a stand in their interests."

"And the months ahead, the years ahead it's only going to get worse until eventually there will be a time where policies will change because the only thing that restricts the activities of the surveillance state are policy. Even our agreements with other sovereign governments, we consider that to be a stipulation of policy rather then a stipulation of law. And because of that a new leader will be elected, they'll find the switch, say that 'Because of the crisis, because of the dangers we face in the world, some new and unpredicted threat, we need more authority, we need more power.' And there will be nothing the people can do at that point to oppose it. And it will be turnkey tyranny."

Gabriel Rodriguez
Gabriel Rodriguez is currently studying for a Masters in Applied Economics at Georgetown. He is a graduate of New College of Florida with a degree in Economics. He is interested in behavioral economics, development economic, fishing economics, and ...
Follow @Zikan

Exhibit 2

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 VERIZON BUSINESS NETWORK SERVICES,
INC. ON BEHALF OF MCI COMMUNICATION
SERVICES, INC. D/B/A VERIZON
BUSINESS SERVICES.

Docket Number: BR

13-80

SECONDARY ORDER

This Court having found that the Application of the Federal Bureau of Investigation (FBI) for an Order requiring the production of tangible things from **Verizon Business Network Services, Inc. on behalf of MCI Communication Services Inc., d/b/a Verizon Business Services (individually and collectively "Verizon")** satisfies the requirements of 50 U.S.C. § 1861,

IT IS HEREBY ORDERED that, the Custodian of Records shall produce to the National Security Agency (NSA) upon service of this Order, and continue production

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

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" created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls. This Order does not require Verizon to produce telephony metadata for communications wholly originating and terminating in foreign countries. 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.

IT IS FURTHER ORDERED that no person shall disclose to any other person that the FBI or NSA has sought or obtained tangible things under this Order, other than to: (a) those persons to whom disclosure is necessary to comply with such Order; (b) an attorney to obtain legal advice or assistance with respect to the production of things in response to the Order; or (c) other persons as permitted by the Director of the FBI or the Director's designee. A person to whom disclosure is made pursuant to (a), (b), or (c)

shall be subject to the nondisclosure requirements applicable to a person to whom an Order is directed in the same manner as such person. Anyone who discloses to a person described in (a), (b), or (c) that the FBI or NSA has sought or obtained tangible things pursuant to this Order shall notify such person of the nondisclosure requirements of this Order. At the request of the Director of the FBI or the designee of the Director, any person making or intending to make a disclosure under (a) or (c) above shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

IT IS FURTHER ORDERED that service of this Order shall be by a method agreed upon by the Custodian of Records of Verizon and the FBI, and if no agreement is reached, service shall be personal.

-- *Remainder of page intentionally left blank.* --

This authorization **requiring the production of certain call detail records or "telephony metadata" created by Verizon** expires on the 19th day of July, 2013, at 5:00 p.m., Eastern Time.

Signed 04-25-2013 P02:26 Eastern Time
Date Time

ROGER VINSON
Judge, United States Foreign
Intelligence Surveillance Court

Exhibit 3

~~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]

Docket Number: BR 13-158

MEMORANDUM

The Court has today issued the Primary Order appended hereto granting the "Application for Certain Tangible Things for Investigations to Protect Against International Terrorism" ("Application"), which was submitted to the Court on October

10, 2013, by the Federal Bureau of Investigation ("FBI"). The Application requested the issuance of orders pursuant to 50 U.S.C. § 1861, as amended (also known as Section 215 of the USA PATRIOT Act), requiring the ongoing daily production to the National Security Agency ("NSA") of certain telephone call detail records in bulk.

The Primary Order appended hereto renews the production of records made pursuant to the similar Primary Order issued by the Honorable Claire V. Eagan of this Court on July 19, 2013 in Docket Number BR 13-109 ("July 19 Primary Order"). On August 29, 2013, Judge Eagan issued an Amended Memorandum Opinion setting forth her reasons for issuing the July 19 Primary Order ("August 29 Opinion"). Following a declassification review by the Executive Branch, the Court published the July 19 Primary Order and August 29 Opinion in redacted form on September 17, 2013.

The call detail records to be produced pursuant to the orders issued today in the above-captioned docket are identical in scope and nature to the records produced in response to the orders issued by Judge Eagan in Docket Number BR 13-109. The records will be produced on terms identical to those set out in Judge Eagan's July 19 Primary Order and for the same purpose, and the information acquired by NSA through the production will be subject to the same provisions for oversight and identical restrictions on access, retention, and dissemination.

This is the first time that the undersigned has entertained an application requesting the bulk production of call detail records. The Court has conducted an independent review of the issues presented by the application and agrees with and adopts Judge Eagan's analysis as the basis for granting the Application. The Court writes separately to discuss briefly the issues of "relevance" and the inapplicability of the Fourth Amendment to the production.

Although the definition of relevance set forth in Judge Eagan's decision is broad, the Court is persuaded that that definition is supported by the statutory analysis set out in the August 29 Opinion. That analysis is reinforced by Congress's re-enactment of Section 215 after receiving information about the government's and the FISA Court's interpretation of the statute. Although the existence of this program was classified until several months ago, the record is clear that before the 2011 re-enactment of Section 215, many Members of Congress were aware of, and each Member had the opportunity to learn about, the scope of the metadata collection and this Court's interpretation of Section 215. Accordingly, the re-enactment of Section 215 without change in 2011 triggered the doctrine of ratification through re-enactment, which provides a strong reason for this Court to continue to adhere to its prior interpretation of Section 215. See Lorillard v. Pons, 434 U.S. 575, 580 (1978); see also EEOC v. Shell Oil Co., 466 U.S. 54, 69 (1984); Haig v. Agee, 453 U.S. 280, 297-98 (1981).

The undersigned also agrees with Judge Eagan that, under Smith v. Maryland, 442 U.S. 735 (1979), the production of call detail records in this matter does not constitute a search under the Fourth Amendment. In Smith, the Supreme Court held that the use of a pen register to record the numbers dialed from the defendant's home telephone did not constitute a search for purposes of the Fourth Amendment. In so holding, the Court stressed that the information acquired did not include the contents of any communication and that the information was acquired by the government from the telephone company, to which the defendant had voluntarily disclosed it for the purpose of completing his calls.

The Supreme Court's more recent decision in United States v. Jones, — U.S. —, 132 S. Ct. 945 (2012), does not point to a different result here. Jones involved the acquisition of a different type of information through different means. There, law enforcement officers surreptitiously attached a Global Positioning System (GPS) device to the defendant's vehicle and used it to track his location for 28 days. The Court held in Justice Scalia's majority opinion that the officers' conduct constituted a search under the Fourth Amendment because the information at issue was obtained by means of a physical intrusion on the defendant's vehicle, a constitutionally-protected area. The majority declined to decide whether use of the GPS device, without the physical intrusion, impinged upon a reasonable expectation of privacy.

Five Justices in Jones signed or joined concurring opinions suggesting that the precise, pervasive monitoring by the government of a person's location could trigger Fourth Amendment protection even without any physical intrusion. This matter, however, involves no such monitoring. Like Smith, this case concerns the acquisition of non-content metadata other than location information. See Aug. 29 Op. at 29 at 4 n.5; id. at 6 & n.10.

Justice Sotomayor stated in her concurring opinion in Jones that it "may be necessary" for the Supreme Court to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties," which she described as "ill suited to the digital age." See Jones, 132 S. Ct. at 957 (Sotomayor, J., concurring) (citing Smith and United States v. Miller, 425 U.S. 435, 443 (1976), as examples of decisions relying upon that premise). But Justice Sotomayor also made clear that the Court undertook no such reconsideration in Jones. See id. ("Resolution of these difficult questions in this case is unnecessary, however, because the Government's physical intrusion on Jones' Jeep supplies a narrower basis for decision."). The Supreme Court may some day revisit the third-party disclosure principle in the context of twenty-first century communications technology, but that day has not arrived. Accordingly, Smith remains controlling with respect to the acquisition by the government from service providers of non-content telephony

metadata such as the information to be produced in this matter.

In light of the public interest in this matter and the government's declassification of related materials, including substantial portions of Judge Eagan's August 29 Opinion and July 19 Primary Order, the undersigned requests pursuant to FISC Rule 62 that this Memorandum and the accompanying Primary Order also be published and directs such request to the Presiding Judge as required by the Rule.

ENTERED this 11th day of October, 2013.

Mary A. McLaughlin

MARY A. McLAUGHLIN
Judge, United States Foreign
Intelligence Surveillance Court

[redacted]

~~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]

Docket Number: BR 13-158

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: [redacted]

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 BR 13-109 and its predecessors. [50 U.S.C. § 1861(c)(1)]

Accordingly, and as further explained in the accompanying Memorandum, 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"[1] created by [redacted]

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

[1] 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. Furthermore, this Order does not authorize the production of cell site location information (CSLI).

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]

(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.[2] The BR metadata shall carry unique markings such

[2] 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.[3] 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[4] 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.

[3] 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 queries of the BR metadata to obtain contact chaining information as described in paragraph 17 of the Declaration o[redacted] [redacted] attached to the application as Exhibit A, using selection terms approved as "seeds" pursuant to the RAS approval process described below.[5] NSA shall ensure,

[5] 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.

through adequate and 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.[6]

(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]

[6] This auditable record requirement shall not apply to accesses of the results of RAS-approved queries.

[redacted]

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

[redacted]

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] solely 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] 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.[9,10]

---

[9] 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.

[10] The Court understands that NSA receives certain call detail records pursuant to other authority, in addition to the call detail records produced in response to this Court's Orders. NSA shall store, handle, and disseminate call detail records produced in response to this Court's Orders pursuant to this Orde[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.[11] 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]

[11] This automated query process was initially approved by this Court in its November 8, 2012 Order amending docket number BR 12-178.

[12] 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]

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]

receive appropriate and adequate training and guidance regarding the procedures and restrictions for the handling and dissemination of such information.[15] 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.[16] 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

[15] 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.

[16] 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.[17] OGC shall provide NSD/DoJ with copies

[17] 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) Other than the automated query process described in the [redacted] Declaration and this Order, prior to implementation of any new or modified automated query processes, such new or modified 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 and operation 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] expires on the 3RD day of January, 2014, at 5:00 p.m., Eastern Time.

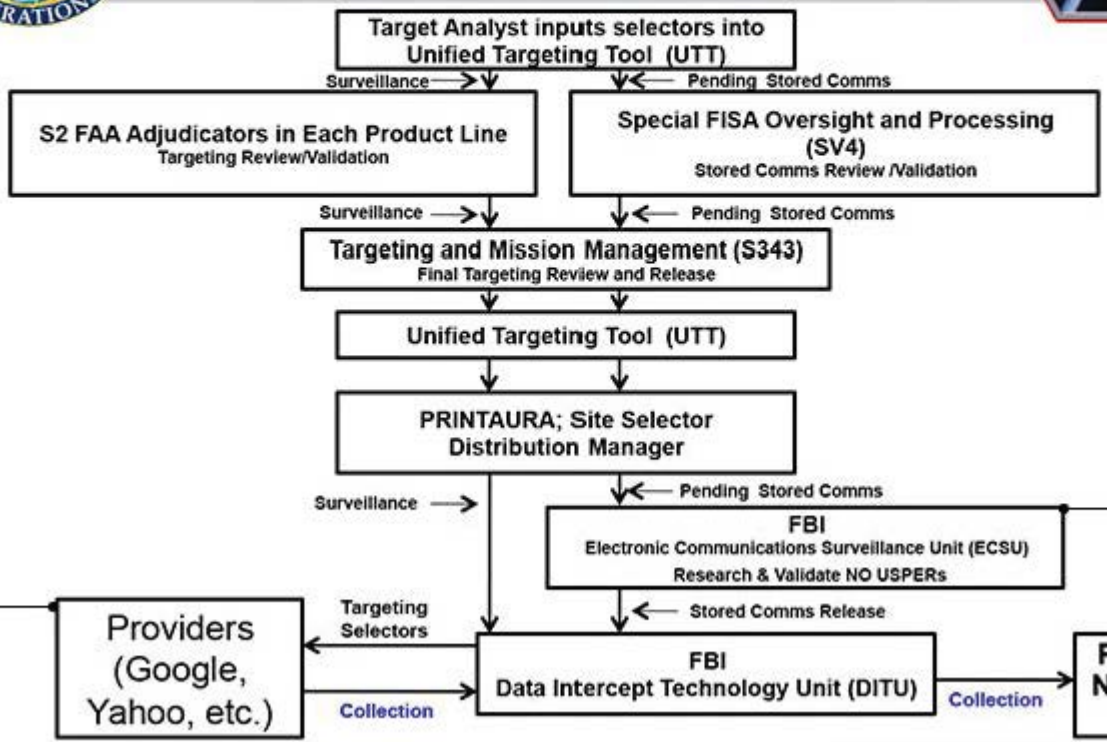
Signed 10-11-2013 P12:05 Eastern Time
Date Time

Mary A. McLaughlin
MARY A. MCLAUGHLIN
Judge, United States Foreign
Intelligence Surveillance Court

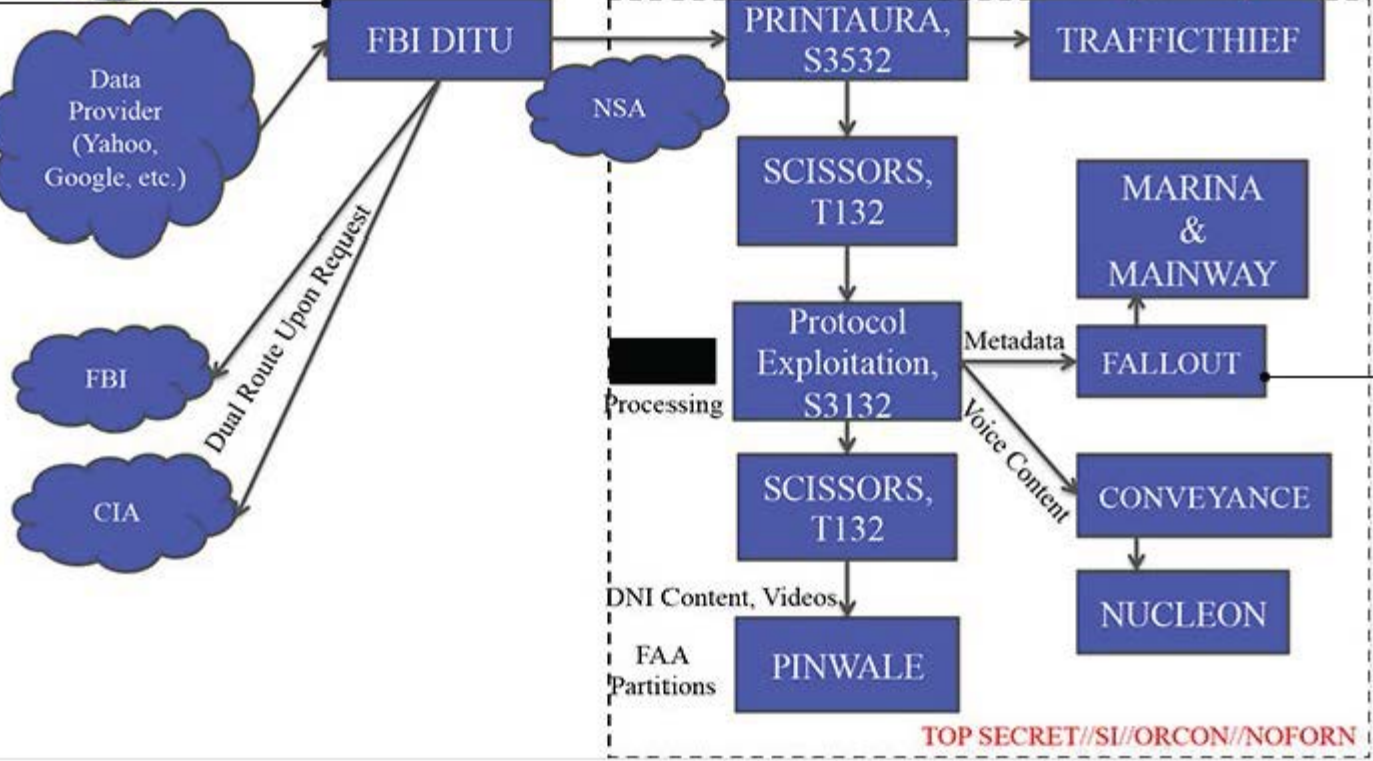
[redacted]

Exhibit 4

(TS//SI//NF) PRISM Tasking Process



(TS//SI//NF) PRISM Collection Dataflow



(TS//SI//NF) PRISM Case Notations

P2ESQC120001234

PRISM Provider
- P1: Microsoft
- P2: Yahoo
- P3: Google
- P4: Facebook
- P5: PalTalk
- P6: YouTube
- P7: Skype
- P8: AOL
- PA: Apple

Fixed trigraph, denotes PRISM source collection

Year CASN established for selector

Serial #

Content Type
- A: Stored Comms (Search)
- B: IM (chat)
- C: RTN-EDC (real-time notification of an e-mail event such as a login or sent message)
- D: RTN-IM (real-time notification of a chat login or logout event)
- E: E-Mail
- F: VoIP
- G: Full (WebForum)
- H: OSN Messaging (photos, wallposts, activity, etc.)
- I: OSN Basic Subscriber Info
- J: Videos
- . (dot): Indicates multiple types

TOP SECRET//SI//ORCON//NOFORN

(TS//SI//NF) REPRISMFISA TIPS

(https:[redacted]

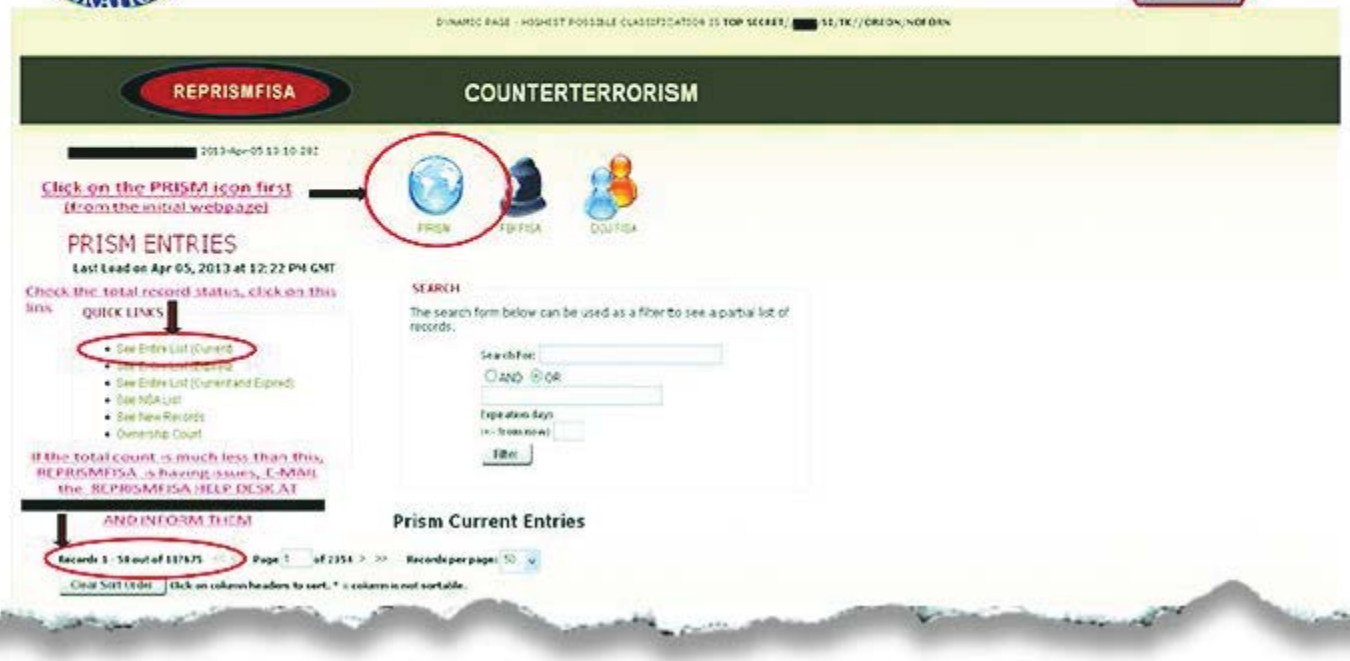


Exhibit 5

(U//FOUO) WINDSTOP/2P
System Highlights

MUSCULAR

- Minor circuit move, not collection suite move (so-2013-00762)
- XKS FP updates across TU systems / NArchive throttle update

INCENSER

- INCS4 config issue (uo-2013-00471)

Speaker's Notes

From Feb 28 2013: Proposed/imminent latest DO/Volume reduction: Narchive

BLUF: Requested S2 concurrence at S2 TLC on 25 Feb with partial throttling of content from Yahoo, Narchive email traffic which contains data older than 6 months from MUSCULAR. Numerous S2 analysts have complained of its existence, and the relatively small intelligence value it contains does not justify the sheer volume of collection at MUSCULAR (1/4th of the total daily collect).

Background: Since July of 2012, Yahoo has been transferring entire email accounts using the Narchive data format (a proprietary format for which NSA had to develop custom demultiplexers). To date, we are unsure why these accounts are being transferred – movement of individuals, backup of data from overseas servers to US servers, or some other reason. There is no way currently to predict if an account will be transferred via Yahoo Narchive.

Currently, Narchive traffic is collected and forwarded to NSA for memorialization in any quantity only from DS-200B. On any given day, Narchive traffic represents 25% (15GB) of DS-200B's daily PINWALE content allocation (60GB currently). DS-200B is scheduled to be upgraded in the summer of 2013; it is likely that memorialized Narchive traffic, if still present in the environment, will grow proportionally (i.e. double now, to 30 GB/day).

Narchive traffic is mailbox formatted email, meaning unlike Yahoo webmail, any attachments present would be collected as part of the message. This is a distinct advantage. However, it has not been determined what causes an Narchive transfer of an account, so these messages are rarely collected "live".

Based on analysis of Narchive email data by [redacted] and [redacted], we were able to indentify statistics for the original communications date for Narchive email messages collected:

< 30 days	1118	11%
> 30 days, < 90 days	1758	17%
> 90 days < 180 days	1302	13%
> 180 days, < 1 year	2592	26%
> 1years, < 5 years	3084	31%
> 5years	154	>1%

Numerous target offices have complained about this collection "diluting" their workflow. One argument for keeping it is that it provides a retrospective look at target activity – this argument is hampered by a) the unreliable and non-understood nature of when the transfer occurs for an account, and b) that FISA restrospective collection would retrieve the exact same data "on demand".

SSO Optimization believes that while this is "valid" collection of content, the sheer volume and the age – coupled with the unpredictable nature of Narchive activity – makes collecting older data a less desirable use of valuable resources. 59% of Narchive email collected was originally sent and received more than 180 days after collection. This represents about 8.9 GB a day of "less desirable" collection – long term allocation that could be easily filled with more timely, useful FI from this lucrative SSO site. As always with our optimization, the data would still be available at the site store for SIGDEV. This would not impact metadata extraction.

Past DO volume reduction efforts:
Webmail OAB- Leap day 2012: the original defeat only targeted gmail, yahoo, and hotmail webmail protocol
FB buddylist sampling since last year

Today: FB OAB defeat/atxks/facebook/ownerless_addressbook : this is a JSON addressbook

Exhibit 6

Content Acquisition Optimization

[redacted]

Yahoo Webmessenger

- Update data sent to individuals logged into Yahoo's Instant Messenger service online
  - Online contact status, unread emails in Yahoo inbox
  - Usually small sessions (2-4kB)
- Sporadic collection (30,000 – 60,000 sessions per day)
- Intermittent bursts of collection against contacts of targets
  - Large numbers of sessions (20,000+) against a single targeted selector
  - Not collected against the target (online presence/unread email from target)
  - No owner attribution (metadata value limited to fact-of comms for emails, online presence events for buddies)
- Over a dozen selectors detasked in two weeks
  - Because a target's contact was using/idling on Yahoo Webmessenger
  - Several very timely selectors (Libyan transition, Greek financial related)

Address Books

- Email address books for most major webmail are collected as stand-alone sessions (no content present*)
- Address books are repetitive, large, and metadata-rich
- Data is stored multiple times (MARINA/MAINWAY, PINWALE, CLOUDs)
- Fewer and fewer address books attributable to users, targets
- Address books account for ~ 22% of SSO's major accesses (up from ~ 12% in August)

Access (10 Jan 12)	Total Sessions	Address Books
US-3171	1488453	237067 (16% of traffic)
DS-200B	938378	311113 (33% of traffic)
US-3261	94132	2477 (3% of traffic)
US-3145	177663	29336 (16% of traffic)
US-3180	269794	40409 (15% of traffic)
US-3180 (16 Dec 11)	289318	91964 (32% of traffic)
TOTAL	3257738	712366 (22% of traffic)

Provider	Collected	Attributed	Attributed%
Yahoo	444743	11009	2.48%
Hotmail	105068	1115	1.06%
Gmail	33697	2350	6.97%
Facebook	82857	79437	95.87%
Other	22881	1175	5.14%
TOTAL	689246	95086	13.80%

Buddy Lists,Inboxes

- Unlike address books, frequently contain content data
  - Offline messages, buddy icon updates, other data included
  - Webmail inboxes increasingly include email content
  - Most collection is due to the presence of a target on a buddy list where the communication is **not** to, from, or about that target

- NSA collects, on a representative day, ~ 500,000 buddylists and inboxes
  - More than 90% collected because tasked selectors identified only as contacts (not communicant, content, or owner)

- Identifying buddylists and inboxes without content (or without useful content) an ongoing challenge

Scenario: [redacted]@yahoo

- [redacted] Sep 2011 [redacted]@yahoo.com (tasked S2E, asw Iran Quds Force) has his/her Yahoo account hacked by an unknown actor, sends out spam email to his/her contact list:

DNI Parser Webmail Display YAHOO! MAIL Active user: [redacted]

Message	
Date	2011-09-[redacted]
Subject	[redacted]!!!!! (New)
From	[redacted]@yahoo.com>
To	[redacted]@yahoogroups.com

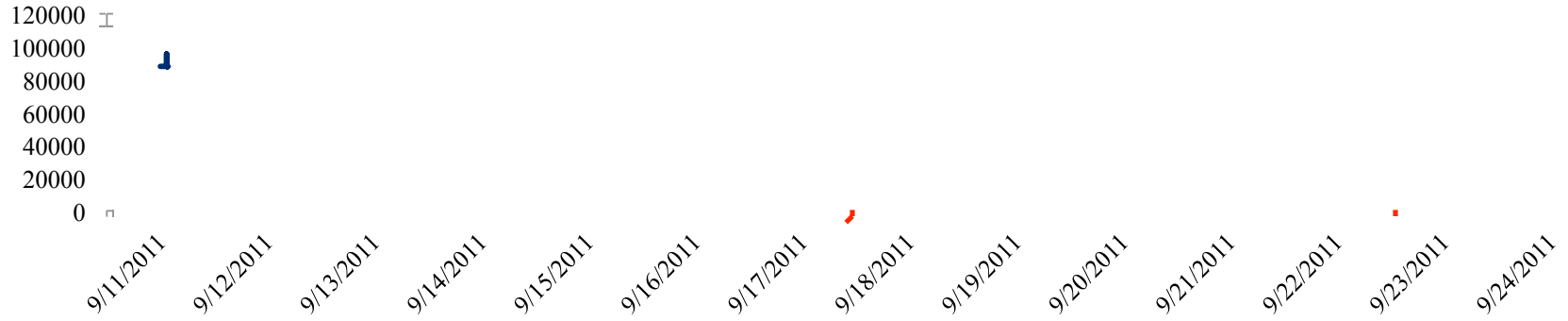
[redacted]

Scenario: [redacted]@yahoo

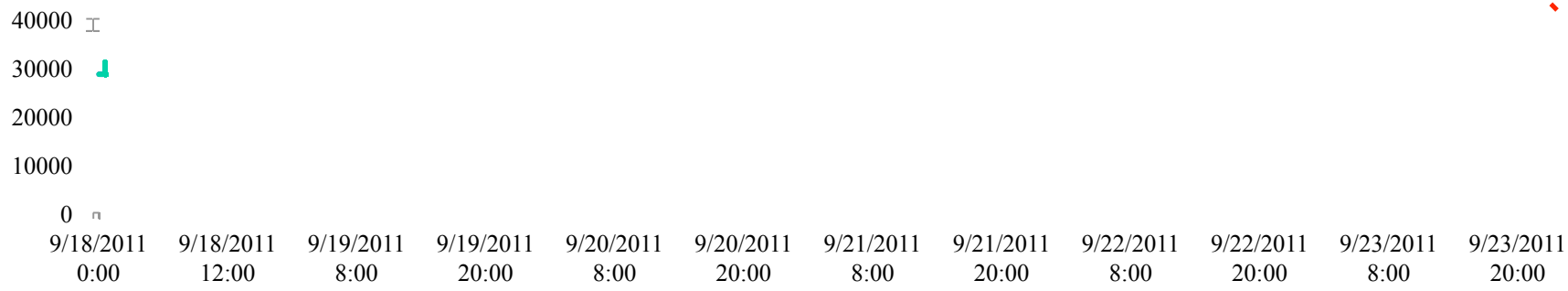
- [redacted]@yahoo.com has a number of Yahoo groups in his/her contact list, some with many hundreds or thousands of members
- At DS-200B in particular, collection spiked as:
  - The initial spam messages were sent (and collected)
  - Inboxes of email recipients were viewed by [redacted] contact list
  - Messages were sometimes viewed, but more often sent as precached views on Google and Yahoo (along with inboxes)
  - Inboxes where the recipient did not delete the spam message continued to be collected every time they were viewed
  - Some recipients added [redacted]@yahoo.com to their address books (possibly as a spam defeat?) – address books were collected every time

Scenario: [redacted]@yahoo

DS-200B Collection By Day - 11 Sep - 24 Sep (in MB)



DS-200B Collection By Hour – 18 Sep – 23 Sep (in MB)



Scenario: [redacted]@yahoo

- [redacted]@yahoo.com emergency detasked from DS-200B and US-3171 at 13:04Z on 20 Oct
- Numerous first-order address books and inboxes collected meant tasked selectors on address books or buddy lists of contacts of [redacted]@yahoo.com also affected:
  - [redacted]@yahoo.com and [redacted]@gmail.com emergency detasked off US-3171 at 13:10Z on 20 Sep
- Memorializing to PINWALE only address books and inboxes owned by target selectors would have reduced PINWALE volumes 90%+
  - Site XKEYSCOREs would buffer data for SIGDEV purposes
  - Metadata from known owner address books and inboxes stored regardless

Mobile IMAP

- IMAP protocol used by email clients to fetch mail from server(s)
- Not designed for devices with intermittent connections (i.e. mobile phones)
- Android implementation in particular uses a lot of bandwidth

```
A0 CAPABILITY
A1 LOGIN [redacted]
A2 CAPABILITY
A3 EXAMINE INBOX
A4 LIST "" INBOX
A5 LIST "" "INBOX.%"
A6 SEARCH SINCE 15-Aug-2011 UNDELETED ALL
A7 FETCH 17 (ENVELOPE INTERNALDATE RFC822.SIZE
A8 FETCH 17 (BODY.PEEK[HEADER])
A9 CLOSE
A10 LOGOUT
```

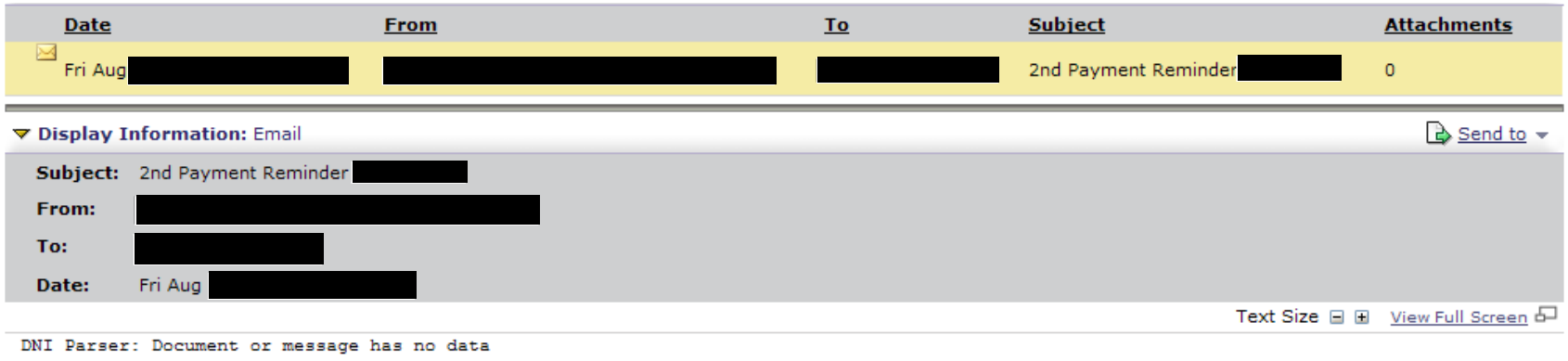


Exhibit 7

UNITED STATES GOVERNMENT

Memorandum

OC-034-12

DATE: 3 May 2012

REPLY TO ATTN OF: SID Oversight & Compliance

SUBJECT: (U//FOUO) NSAW SID Intelligence Oversight (IO) Quarterly Report – First Quarter Calendar Year 2012 (1 January – 31 March 2012) – EXECUTIVE SUMMARY

TO: SIGINT Director

I. (U) Overview

(U//FOUO) The attached NSAW SID Intelligence Oversight (IO) Quarterly Report for the First Quarter Calendar Year 2012 (1 January – 31 March 2012) identifies NSAW SID compliance with E.O. 12333, DoD Regulation 5240.1-R, NSA/CSS Policy 1-23, USSID SP0018, and all related policies and regulations.

(U//FOUO) Detailed incident narratives are provided in the attached annexes. The number of incidents in each category and a reference to the annex related to each incident category are contained in the body of the report.

(U//FOUO) As part of SID Oversight and Compliance's (SV) charge to provide comprehensive trends and analysis information as it pertains to incidents of non-compliance, this Executive Summary provides analysis and evaluation of incidents reported throughout the current quarter to better address the "whys" and "hows" behind NSAW SID's compliance posture.

(U//FOUO) Section II, Metrics, has been broken down into several sub-sections: metrics and analysis of NSAW SID-reported incidents by authority, type, root cause, and organization. Also included is an assessment of how incidents were discovered (i.e., methods of discovery) for SID-reported incidents (see **Figure 7**).

(U//FOUO) Significant Incidents of Non-compliance and Report Content follow in Sections III and IV, respectively.

(S//REL) Overall, the number of incidents reported during 1QCY12 increased by 11% as compared to the number of incidents reported during 4QCY11. This included a rise in the number of E.O. 12333 incidents, as well as for incidents across all FISA authorities. The majority of incidents in all authorities were database query incidents due to human error. Of note, S2 continued to be the NSAW SID organization with the largest number of reported incidents (89%), although S2 experienced an overall decrease in reported incidents. SV noted an overall improvement in timeliness regarding 1QCY12 IO Quarterly Report submissions from the SID elements.

II. (U) Metrics

a. (U//FOUO) NSAW SID-reported Incidents by Authority

(TS//SI//REL TO USA, FVEY) **Figures 1a-b** compares all categories of NSAW SID-reported incidents (collection, dissemination, unauthorized access, and retention) by Authority for 2QCY11 – 1QCY12. From 4QCY11 to 1QCY12, there was an overall increase in incidents of 11%. There was also an increase of 11% for both E.O. 12333 and FISA incidents. The increase in incidents reported for 1QCY12 was due to an increase in the number of reported Global System for Mobile Communications (GSM) roamer[1] incidents, which may be attributed to an increase in Chinese travel to visit friends and family for the Chinese Lunar New Year holiday.

(U//FOUO) **Figure 1a**: Table of the Number of NSAW SID-reported Incidents by Authority

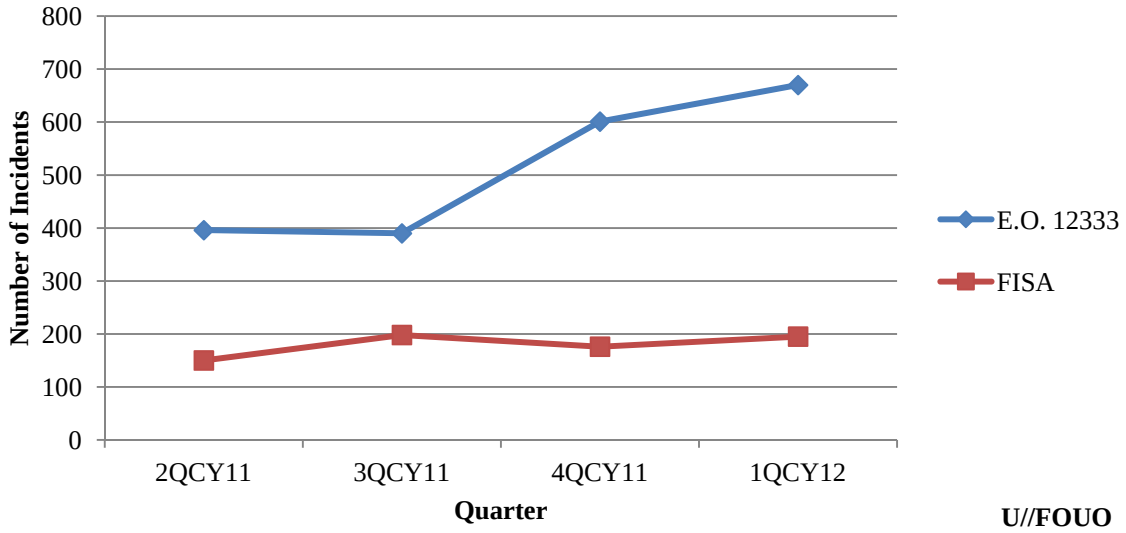
(U//FOUO)

	2QCY11	3QCY11	4QCY11	1QCY12
E.O. 12333	396	390	601	670
FISA	150	198	176	195
TOTAL	**546**	**588**	**777**	**865**

(U//FOUO)

(U//FOUO) **Figure 1b**: Line Graph of the Number of NSAW SID-reported Incidents by Authority

U//FOUO



U//FOUO

(TS//SI//NF) **FISA Incidents:** As reflected in **Figures 1a-b**, during 1QCY12, NSAW SID reported a total of 195 FISA incidents, 185 of which were associated with unintentional collection. NSAW SID also reported 6 incidents of unintentional dissemination under FISA authority and 4 incidents of unauthorized access to Raw

[1] (U//FOUO) Roaming incidents occur when a selector associated with a valid foreign target becomes active in the U.S.

SIGINT FISA data. **Figure 2** illustrates the most common root causes for incidents involving FISA authorities as determined by SV.

- 63% (123) of 1QCY12 FISA incidents can be attributed to Operator Error as the root cause, and involved:
  - Resources (i.e., inaccurate or insufficient research information and/or workload issues (60);
  - Lack of due diligence (i.e., failure to follow standard operating procedures) (39);
  - Human error (21) which encompassed:
    - Broad syntax (i.e., no or insufficient limiters / defeats / parameters) (12);
    - Typographical error (6);
    - Query technique understood but not applied (2); and
    - Incorrect option selected in tool (1); and
  - Training and guidance (i.e., training issues) (3).

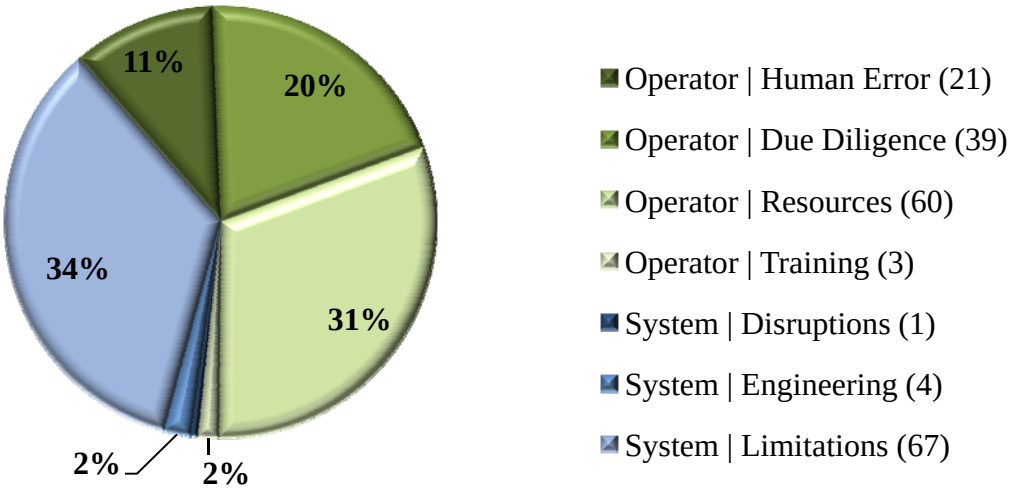
(U//FOUO) The Resources root cause category accounted for the largest percentage of Operator Error incidents under FISA authorities for 1QCY12. Analysis identified that these incidents could be reduced if analysts had more complete and consistent information available about selectors and/or targets at the time of tasking and if analysts consistently applied rules for conducting queries.

- 37% (72) of 1QCY12 FISA incidents can be attributed to System Error as the root cause, and involved:
  - System limitations (i.e., system lacks the capability to 'push' real-time travel data out to analysts, system/device unable to detect changes in user) (67);
  - System engineering (i.e., system/database developed without the appropriate oversight measures, data flow issues, etc.) (4); and,
  - System disruptions (i.e., glitches, bugs, etc.) (1).

(U//FOUO) The System Limitations root cause category accounted for the largest percentage of System Error incidents under FISA authorities for 1QCY12. The largest number of incidents in the System Limitations category account for roamers where there was no previous indications of the planned travel. These incidents are largely unpreventable. Consistent discovery through the Visitor Location Register (VLR) occurs every quarter and provides analysts with timely information to place selectors into candidate status or detask. Analysis identified that these incidents could be reduced if analysts removed/detasked selectors more quickly upon learning that the status of the selector had changed and more regularly monitored target activity. This analysis indicates that continued research on ways to exploit new technologies and researching the various aspects of personal communications systems to include GSM, are an important step for NSA analysts to track the travel of valid foreign targets.

(U//FOUO) **Figure 2**: 1QCY12 FISA Incidents – Root Causes

U//FOUO



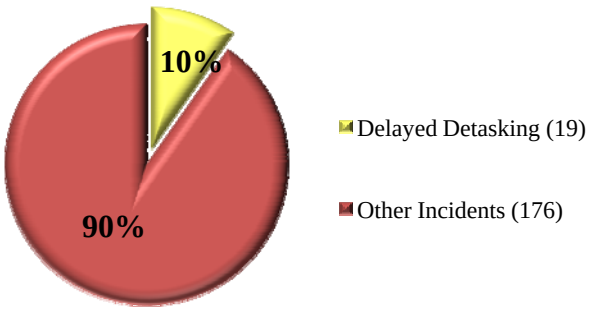
Total: 195

U//FOUO

(TS//SI//REL TO USA, FVEY) Delayed Detasking **FISA Incidents:** As reflected in **Figures 1a-b**, during 1QCY12, NSAW SID reported a total of 195 FISA incidents. 19 (10%) of the total FISA incidents were associated with detasking delays. Of the 19 delayed detasking incidents, 12 (63%) of these incidents occurred under NSA FISA Authority, 5 (27%) occurred under FAA 702 Authority, 1(5%) occurred under FAA 704 Authority, and 1 (5%) occurred under FAA 705(b) Authority. **Figure 3a** illustrates the detasking delay incidents versus all other FISA incidents reported during 1QCY12. **Figure 3b** illustrates the detasking delay incidents by FISA Authority reported during 1QCY12.

(U//FOUO) Figure 3a: 1QCY12 Detasking FISA Incidents vs. All other FISA incidents

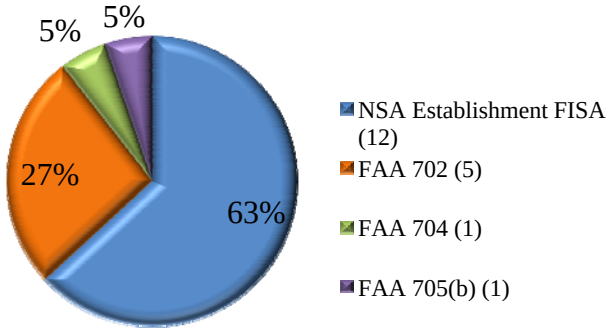
U//FOUO



Total: 195

(U//FOUO) Figure 3b: 1QCY12 FISA Incidents by Authority – Delayed Detaskings

U//FOUO



Total: 19

U//FOUO

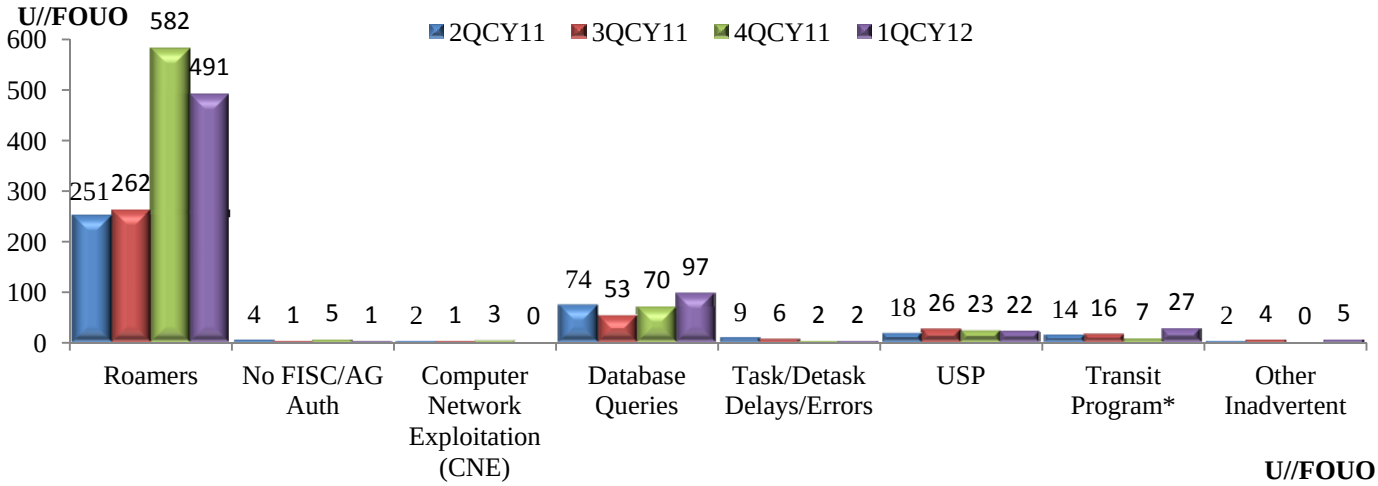
U//FOUO

(TS//SI//REL TO USA, FVEY) As depicted in Figures 3a and 3b, of the 19 delayed detasking FISA incidents, 15 (79%) resulted from a failure to detask all selectors, 2 (11%) resulted from analyst not detasking when required, 1 (5%) resulted from partner agency error, and 1 (5%) resulted from all tasking not terminated (e.g., dual route).

b. NSAW SID-reported Collection Incidents by Sub-Type and Authority

(U//FOUO) **Figures 4a-b** depicts NSAW SID-reported collection incidents by Authority (E.O. 12333 and all FISA Authorities), and identifies the primary sub-types for those incidents. An explanation of the more prominent collection incident sub-types follows the graphs.

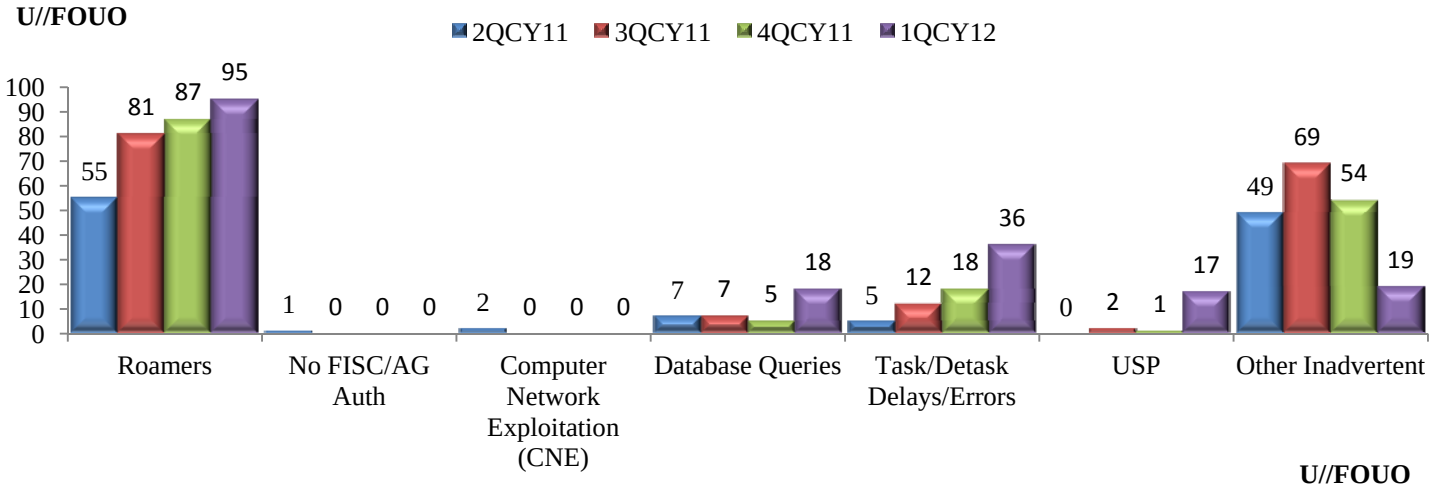
(U//FOUO) **Figure 4a**: NSAW SID-reported Collection Incidents Under E.O. 12333 Authority



(U//FOUO) **Figure 4a:** During 1QCY12, NSAW SID reported a 39% increase of database query incidents under E.O. 12333 Authority. Human Error accounted for 74% of E.O.12333 database query incidents.

(TS//SI//REL TO USA, FVEY) **International Transit Switch Collection*:** International Transit switches, FAIRVIEW (US-990), STORMBREW (US-983), ORANGEBLOSSOM (US-3251), and SILVERZEPHYR (US-3273), are Special Source Operations (SSO) programs authorized to collect cable transit traffic passing through U.S. gateways with both ends of the communication being foreign. When collection occurs with one or both communicants inside the U.S., this constitutes inadvertent collection. From 4QCY11 to 1QCY12, there was an increase of transit program incidents submitted from 7 to 27, due to the change in our methodology for reporting and counting of these types of incidents. (*See Annex G in SID's 1QCY12 IO Quarterly Report for additional details regarding these incidents.)

(U//FOUO) **Figure 4b**: NSAW SID-reported Collection Incidents Under All FISA Authorities



(U//FOUO) **Figure 4b:** During 1QCY12, NSAW SID reported an increase of 9% of roamer incidents under all FISA Authorities. There was also a 260% increase in database query FISA Authority incidents during 1QCY12. Human Error accounted for the majority of all FISA Authorities database query incidents (74%).

(U//FOUO) **Roamers:** Roaming incidents occur when valid foreign target selector(s) are active in the U.S. Roamer incidents continue to constitute the largest category of collection incidents across E.O. 12333 and FAA authorities. Roamer incidents are largely unpreventable, even with good target awareness and traffic review, since target travel activities are often unannounced and not easily predicted.

(S//SI//NF) **Other Inadvertent Collection:** Other inadvertent collection incidents account for situations where targets were believed to be foreign but who later turn out to be U.S. persons and other incidents that do not fit into the previously identified categories.

(TS//SI//REL TO USA, FVEY) **Database Queries:** During 1QCY12, NSAW SID reported a total of 115 database query incidents across all Authorities, representing a 53% increase from 4QCY11. E.O. 12333 Authority database query incidents accounted for 84% (97) of the total, and all FISA Authorities database query incidents accounted for 16% (18).

(U//FOUO) **Figure 5** illustrates the most common root causes for incidents involving database queries as determined by SV.

- 99% (114) of the 1QCY12 database query incidents are attributed to Operator Error as the root cause, and involved:
  - Human error (85) which encompassed:
    - Broad syntax (i.e., no or insufficient limiters / defeats / parameters) (55);
    - Typographical error (17);
    - Boolean operator error (6);
    - Query technique understood but not applied (4);
    - Not familiar enough with the tool used for query (2); and

- Incorrect option selected in tool (1)

- Lack of due diligence (i.e., failure to follow standard operating procedure) (13)
- Training and guidance (i.e., training issues) (9); and
- Resources (i.e., inaccurate or insufficient research information and/or workload issues) (7).

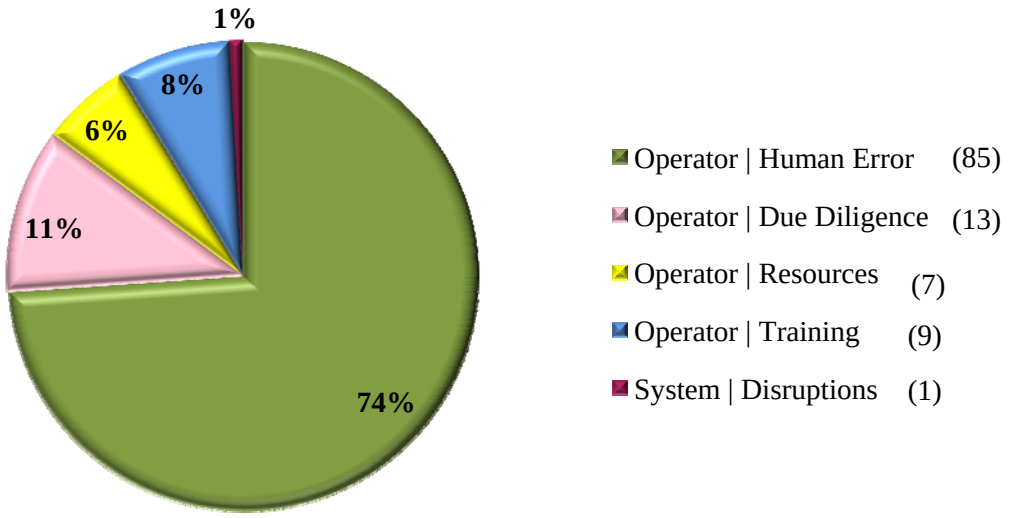
(U//FOUO) The remaining 1 database query incident can be attributed to System Error as the root cause and occurred due to a mechanical error with the tool.

(U//FOUO) Analysis identified that the number of database query incidents could be reduced if analysts more consistently applied rules/standard operating procedures (SOPs) for conducting queries.

(S//SI//NF) Auditors continue to play an important role in the discovery of database query incidents, identifying 70 (61%) of the 115 reported database query incidents.

(U//FOUO) **Figure 5**: 1QCY12 Database Query Incidents – Root Causes

U//FOUO



Total: 115

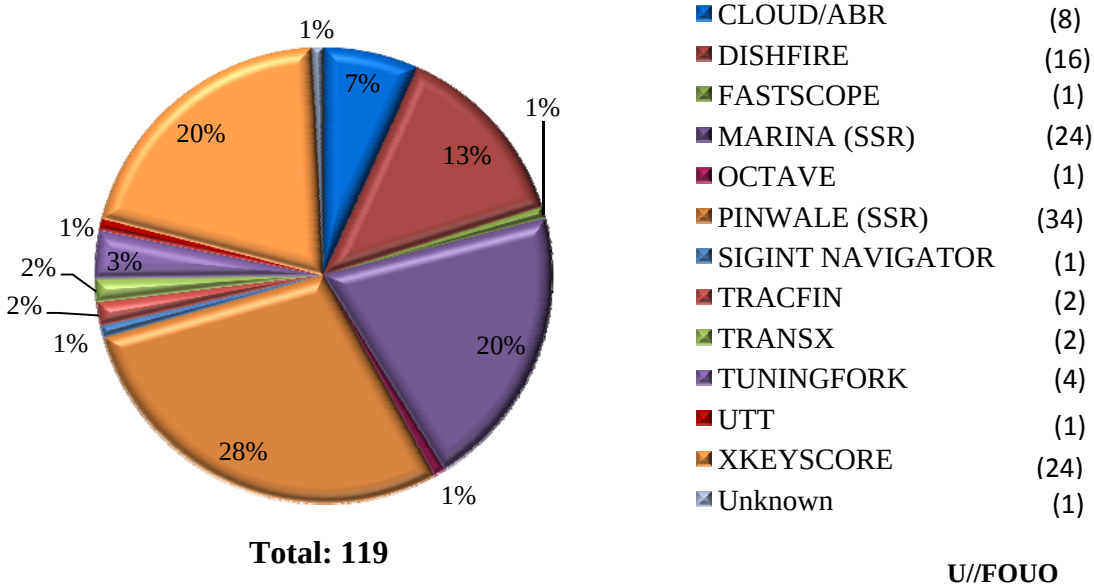
U//FOUO

(TS//SI//REL TO USA, FVEY) Of the 115 database query incidents reported for 1QCY12, **Figure 6** identifies the database involved and the associated percentage of the total. Databases considered to be Source Systems of Record (SSR) have been labeled as such.

(TS//SI//REL TO USA, FVEY) Note that the total number of databases involved in the database query incidents in **Figure 6** does not equal the number of database query incidents reflected in Figure 5 or in the 1QCY12 SID IO Quarterly Report because a database query incident may occur in more than one database.

(U//FOUO) **Figure 6**: 1QCY11 Database Query Incidents – Database(s) Involved

U//FOUO



Total: 119

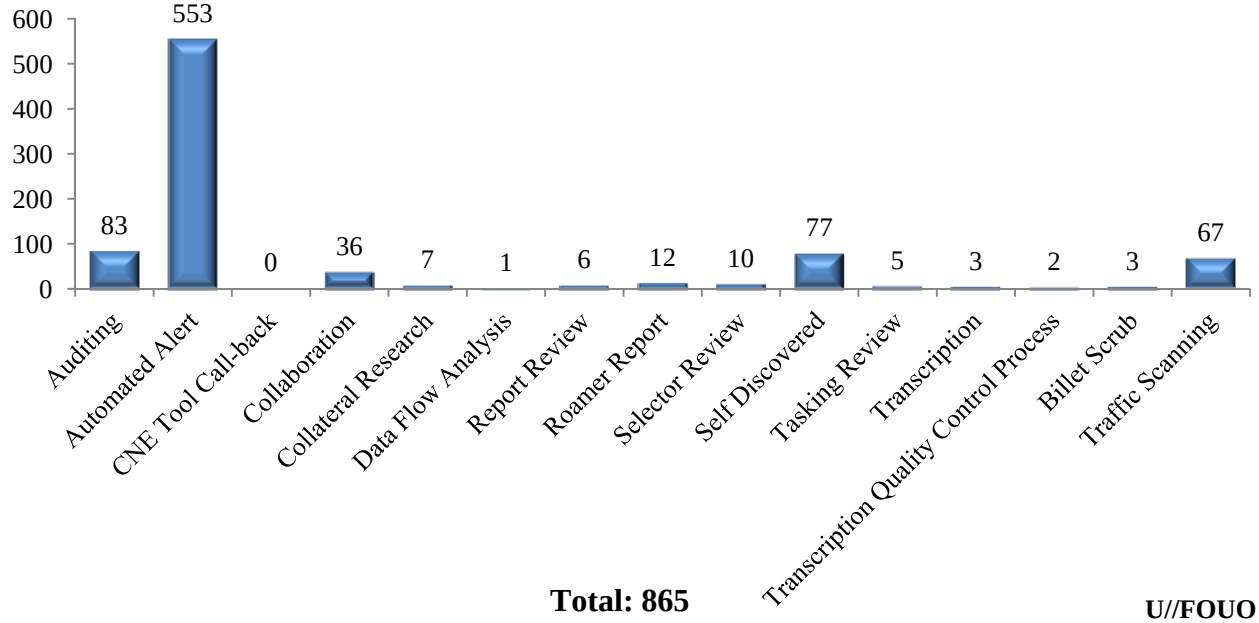
U//FOUO

(U//FOUO) NSAW SID-reported Incidents – Method of Discovery

(U//FOUO) **Figure 7** depicts the most prominent method(s) of discovery for incidents reported by NSAW SID elements for 1QCY12. As SV's assessment of root causes matures, and as corrective measures are implemented, identification of how incidents are discovered will provide additional insight into the effectiveness of those methods.

(U//FOUO) **Figure** 7: 1QCY12 Incidents – How Discovered

U//FOUO



Total: 865

U//FOUO

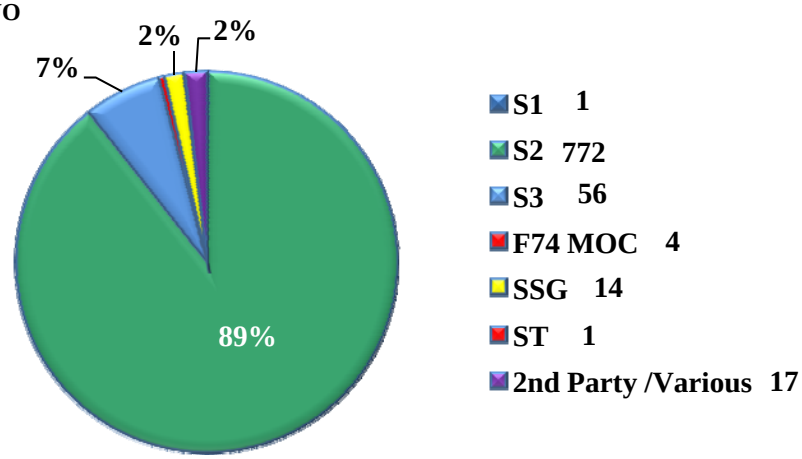
(U//FOUO) For 1QCY12, of the 865 reported incidents, 553 (64%) were discovered by automated alert. 444, (80%) of the 553 incidents that were discovered by automated alert occurred via the VLR and other analytic tools, such as SPYDER, CHALKFUN, and TransX.

c. (U//FOUO) NSAW SID-reported Incidents by Organization

(U//FOUO) **Figure 8** illustrates the total 1QCY12 NSAW SID-reported incidents by primary SID Deputy Directorate (DD) level organization. S2, having the largest NSAW SID contingent of reported incidents, accounted for 89% of the total incidents for the quarter, a proportion consistent with the overall size of the S2 organization. As compared to 4QCY11, S2 experienced an overall 8% reduction in incidents occurrences.

(U//FOUO) **Figure 8**: 1QCY12 Incidents by NSAW SID Organization

U//FOUO



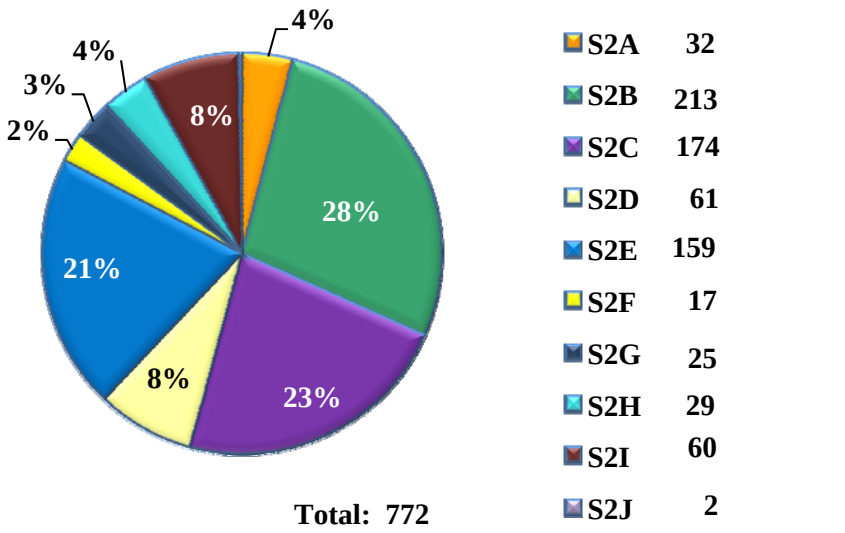
Total: 865

U//FOUO

(U//FOUO) **Figure 9** provides a look into S2 (by Product Line) as the NSAW SID organization with the largest number of reported incidents. For 1QCY12, three Product Lines accounted for 72% of S2's reported incidents. These Product Lines were: the and Korea Division (S2B) with 28% of the reported incidents, the International Security Issues Division (S2C) with 23% of the reported incidents, and the China, and the Office of Middle East & Africa (S2E) with 21% of the incidents. As compared to 4QCY11, this resulted in an increase of 16% for S2B, a reduction of 35% for S2C, and an increase of 9% for S2E. The number of incidents reported by the remaining seven Product Lines held relatively steady from 4QCY11 to 1QCY12.

(U//FOUO) **Figure 9**: 1QCY12 S2 Incidents by Product Line

(U//FOUO)

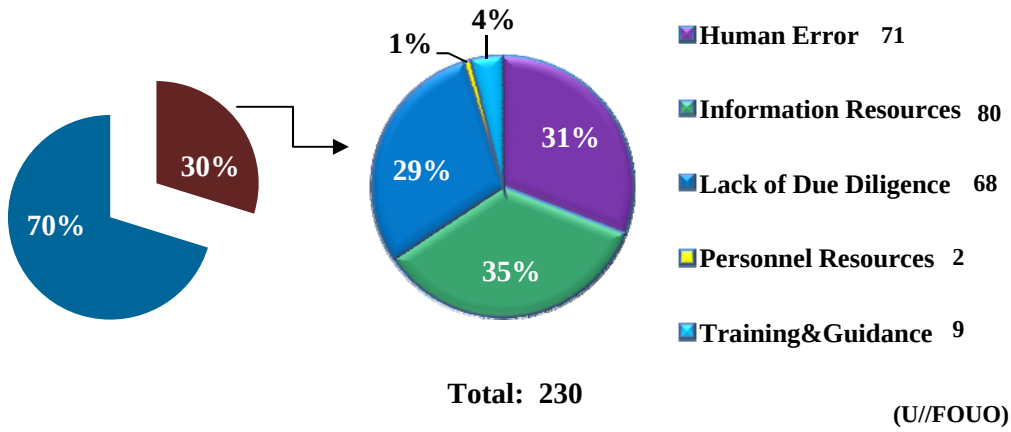


(U//FOUO)

(U//FOUO) **Figures 10a-b** illustrates the operator related (**Figure 10a**) and system related (**Figure 10b**) root causes associated with the 772 incidents reported by S2. 30% of the incidents were due to operator related errors that resulted in an incident. 70% of the incidents were due to system related issues that resulted in an incident.

(U//FOUO) **Figure 10a**: 1QCY12 S2 Incidents – Operator Related Root Causes

(U//FOUO)



(U//FOUO)

(U//FOUO) 30% of the S2-reported incidents during 1QCY12 are attributed to Operator Error as the root cause, and involved:

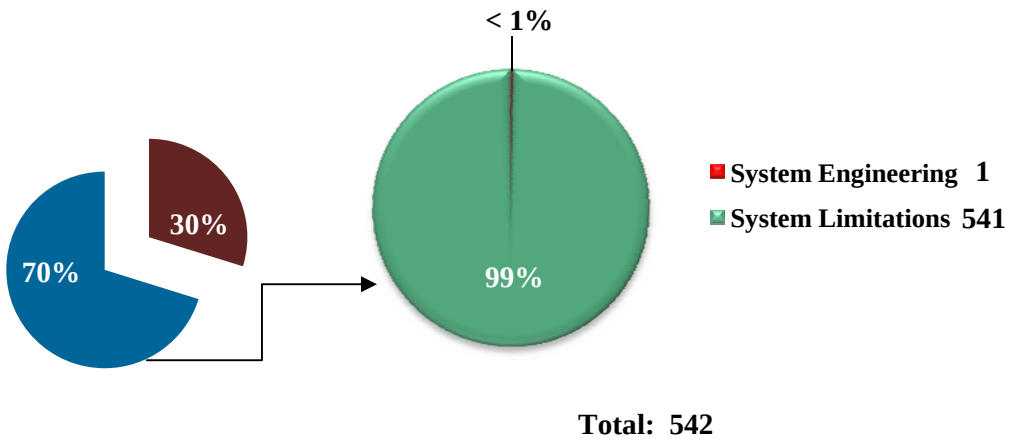
- Resources (i.e., inaccurate or insufficient research information and/or workload issues, and personnel resource issues) (82);

- Human error (i.e., selector mistypes, incorrect realm, or improper query) (71);
- Lack of due diligence (i.e., failure to follow standard operating procedures) (68); and
- Training and guidance (i.e., training issues) (9).

(U//FOUO) Analysis found that analysts could reduce the number of incidents if there was more comprehensive research information available at the time of tasking as well as through better use of defeats, more careful review of data entry to avoid typographical errors and omissions, and by following SOPs more consistently.

(U//FOUO) **Figure 10b**: 1QCY12 S2 Incidents – System Related Root Causes

(U//FOUO)



Total: 542

(U//FOUO)

(U//FOUO) 70% of the S2-reported incidents during 1QCY12 are attributed to system issues as the root cause, and involved:

- System limitations (i.e., system lacks the capability to 'push' real-time travel data out to analysts, system/device unable to detect changes in user) (541); and
- System engineering (i.e., data tagging, configuration, design flaws, etc.) (1).

(TS//SI//REL TO USA, FVEY) System Limitations, the largest percentage of System Error root cause, can be attributed to situations where a valid foreign target is found roaming in the United States without indication in raw traffic.

III. (U) Significant Incidents of Non-compliance

(TS//SI//NF) **Business Record (BR) FISA**. As of 16 February 2012, NSA determined that approximately 3,032 files containing call detail records potentially collected pursuant to prior BR Orders were retained on a server and been collected more than five years ago in violation of the 5-year retention period established for BR collection. Specifically, these files were retained on a server used by technical personnel working with the Business Records metadata to maintain documentation of provider feed data formats and performed background analysis to document why certain contain chaining rules were created. In addition to the BR

work, this server also contains information related to the STELLARWIND program and files which do not appear to be related to either of these programs. NSA bases its determination that these files may be in violation of docket number BR 11-191 because of the type of information contained in the files (i.e., call detail records), the access to the server by technical personnel who worked with the BR metadata, and the listed "creation date" for the files. It is possible that these files contain STELLARWIND data, despite the creation date. The STELLARWIND data could have been copied to this server, and that process could have changed the creation date to a timeframe that appears to indicate that they may contain BR metadata. Additional details regarding this incident can be found in the "Bulk Metadata FISA" Annex, ANNEX R (Item R1) in SID's 1QCY12 IO Quarterly Report.

(S//SI//REL TO USA, FVEY) **Detasking Delay**. Four selectors [redacted] remained active after multiple indications were received that the target held a U.S. green card. On 09 March 2012, a South Asia Language Analysis Branch (S2A51) senior linguist was preparing [redacted] Division) selectors for OCTAVE migration when it was discovered that the tasking record for [redacted] showed that there were four selectors [redacted] that were in active status even though his tasking file indicated he held a U.S. green card as of 03 October 2011. On 09 March 2012, the S2A51 senior linguist detasked the four selectors, and on 13 March 2012, the S2A51 senior linguist requested the 881 cuts in NUCLEON based on collection from those four selectors be purged. On 13 March 2012, a senior reporter in the [redacted] Reporting Branch (S2A52) researched S2A52's locally held file of [redacted] who hold U.S. person status and learned that an S2A52 analyst had indications in intercept on 09 September 201[redacted] might have a U.S. green card. It was also recorded in the same S2A52 file that S2A52 had submitted a request to the Department of Homeland Security (DHS) [redacted] (N.B., the date of the S2A52 request to DHS was not recorded) and learned from DHS on 28 September 2011 that [redacted] had obtained a U.S. green card as of [redacted] 2010. The S2A52 senior reporter then checked ANCHORY and discovered that S2A52 had issued 32 reports between [redacted] 2010 and [redacted] 2011. On 14 March 2012, S2A5 submitted a request for Retroactive Dissemination Authority for the 32 reports which contained the name of [redacted] The Customer Relationships, Information Sharing Services Branch (S12) approved ISS/BDA-068-12 on 16 March 2012. Serialized dissemination of U.S. person information did occur. On 13 March 2012, the S2A51 senior linguist who found that these numbers [redacted] had not been detasked reminded the other two members of the Governmental Unified Targeting Tool (UTT) Group for S2A5 to check all S2A5 databases for [redacted] officials who have U.S. (and Second Party person) status before submitting selectors for tasking. Additional details regarding this incident can be found in the Unintentional Collection under E.O. 12333 Authority Annex, "Collection as a Result of Tasking Errors or Detasking Delays", ANNEX E (Item E1) and in the "Unintentional Dissemination of U.S. Person Information Collected Under E.O. 12333, FISA, and FAA Authorities", Annex M (Item M15) in SID's 1QCY12 IO Quarterly Report.

(C//REL TO USA, FVEY) **Unauthorized Access**. On 29 December 2011, a Cryptanalysis and Exploitation (CES)/Office of Target Pursuit (S31174) Branch Chief discovered that CES personnel had likely been inappropriately granted access to NSA Establishment FISA data. Multiple external factors contributed to this situation. First, in 2002, RAGTIME was changed to encompass both NSA Establishment FISA and FBI FISA, but due to insufficient notice regarding this modification, CES continued to apply the earlier rule that RAGTIME applied only to NSA Establishment FISA data. Second, CES relied on the RAGTIME label in CASPORT for granting access to NSA Establishment FISA data but discovered that CASPORT does not accurately reflect NSA Establishment FISA briefing status. Third, CASPORT often lists NSA-FISA in the

"Oversight" section even though this has nothing to do with a particular user's access. CES has alerted its workforce to look in the CASPORT "Briefing" section for the NSA Establishment FISA entry and CES-controlled software is being updated regarding data access control. Additional details regarding this incident can be found in the "Unauthorized Access to Raw SIGINT" Annex, ANNEX P (Item P2) in SID's 1QCY12 IO Quarterly Report.

(U) Report Content

- **Upcoming Initiatives**

(U//FOUO) During CY12, SV plans to develop 'score cards' to capture and illustrate an organization's reported quarterly activities. SV plans to use this information during scheduled feedback sessions with SID reporting organizations to provide a detailed view into specific areas of high interest or concern arising from analyzing IO Quarterly Report metrics.

- **NSAW SID 1QCY12 IOQ Report Challenges:**

(U//FOUO) SV noted an overall improvement in timeliness regarding 1QCY12 IO Quarterly Report submissions from the SID elements. SV received late submissions from SIGDEV Strategy & Governance (SSG) and SID/Deputy Directorate for Data Acquisition (S3), delaying SV's preparation of the NSAW SID IO Quarterly Report. SV will continue to focus on outreach with SSG and S3 in order to ensure more complete and timely report submissions.

[redacted]
Chief, SID Oversight & Compliance

Exhibit 8

Article

For Immediate Release
August 28, 2013

Grassley Presses for Details about Intentional Abuse of NSA Authorities

WASHINGTON – Senator Chuck Grassley, Ranking Member of the Senate Judiciary Committee, is asking the Inspector General of the National Security Agency (NSA) to provide additional information about the intentional and willful misuse of surveillance authorities by NSA employees. He's also asking for the Inspector General to provide as much unclassified information as possible.

The Senate Judiciary Committee has oversight jurisdiction over the Foreign Intelligence Surveillance Act (FISA) and the intelligence courts that fall under the act's authority.

"The American people are questioning the NSA and the FISA court system. Accountability for those who intentionally abused surveillance authorities and greater transparency can help rebuild that trust and ensure that both national security and the Constitution are protected," Grassley said.

The text of Grassley's letter is below.

August 27, 2013

Dr. George Ellard, Inspector General
National Security Agency
Office of the Inspector General
9800 Savage Road, Suite 6247
Fort Meade, MD 20755

Dear Dr. Ellard:

I write in response to media reports that your office has documented instances in which NSA personnel intentionally and willfully abused their surveillance authorities.

For each of these instances, I request that you provide the following information:

(1) The specific details of the conduct committed by the NSA employee;

(2) The job title and attendant duties and responsibilities of the NSA employee at the time;

(3) How the conduct was discovered by NSA management and/or your office;

(4) The law or other legal authority – whether it be a statute, executive order, or regulation – that your office concluded was intentionally and willfully violated;

(5) The reasons your office concluded that the conduct was intentional and willful;

(6) The specifics of any internal administrative or disciplinary action that was taken against the employee, including whether the employee was terminated; and

(7) Whether your office referred any of these instances for criminal prosecution, and if not, why not?

Thank you for your prompt attention to this important request. I would appreciate a response by September 11, 2013. I also request that you respond in an unclassified manner to the extent possible.

Sincerely,

Charles E. Grassley
Ranking Member

cc: Honorable Patrick Leahy, Chairman

Exhibit 9

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
OFFICE OF THE INSPECTOR GENERAL

11 September 2013

Sen. Charles E. Grassley
Ranking Member
Committee on the Judiciary
United States Senate
152 Dirksen Senate Office Building
Washington, DC 20510

Senator Grassley:

I write in response to your letter of 27 August 2013 requesting information about intentional and willful misuse of surveillance authorities.

Since 1 January 2003, there have been 12 substantiated instances of intentional misuse of the signals intelligence (SIGINT) authorities of the Director of the National Security Agency. The NSA Office of the Inspector General (OIG) currently has two open investigations into alleged misuse of SIGINT and is reviewing one allegation for possible investigation.

1. Civilian Employee, Foreign Location

In 2011, before an upcoming reinvestigation polygraph, the subject reported that in 2004, "out of curiosity," he performed a SIGINT query of his home telephone number and the telephone number of his girlfriend, a foreign national. The SIGINT system prevented the query on the home number because it was made on a US person. The subject viewed the metadata returned by the query on his girlfriend's telephone.

The appropriate OIG conducted an investigation. The subject's actions were found to be in violation of United States Signals Intelligence Directive (USSID) 18 (Legal Compliance and U.S. Person Minimization Procedures).

The matter was referred to DoJ in 2011 for possible violations of 18 U.S.C. §641 (embezzlement and theft) and 18 U.S.C. §2511 (interception and disclosure of electronic communications). In 2011, DoJ declined prosecution. The subject retired in 2012 before disciplinary action had been taken.

2. Civilian Employee, Foreign Location

In 2005, during a pre-retirement reinvestigation polygraph and interview, the subject reported that, in 2003, he tasked SIGINT collection of the telephone number of his foreign-national girlfriend without an authorized purpose for approximately one month to determine whether she was "involved with any [local] government officials or other activities that might get [him] in trouble."

The NSA OIG determined that the subject's actions violated Executive Order 12333, DoD Regulation 5240.1-R, 5 C.F.R. § 2635.704, and NSA/CSS PMM 30-2, Chapter 366, §§ 1-3 and 3-1.

The OIG's report was shared with the NSA Office of General Counsel (OGC) for an assessment as to whether referral to DoJ was appropriate. Records are insufficient to determine whether a referral was made. The subject retired before the OIG investigation was finalized.

3. Civilian Employee, Foreign Location

In 2004, upon her return from a foreign site, the subject reported to NSA Security that, in 2004, she tasked a foreign telephone number she had discovered in her husband's cellular telephone because she suspected that her husband had been unfaithful. The tasking resulted in voice collection of her husband.

The NSA OIG determined that the subject's actions violated USSID 18, Executive Order 12333, 5 C.F.R. §2635.704, and DoD Regulation 5240.1-R, and possibly 18 U.S.C. §2511 (interception and disclosure of electronic communications).

The OIG report was forwarded to NSA's OGC, which referred the matter to DoJ. The subject of the investigation resigned before the proposed discipline of removal was administered

4. Civilian Employee, Foreign Location

In 2003, the appropriate OIG was notified that an employee had possibly violated USSID 18. A female foreign national employed by the U.S. government, with whom the subject was having sexual relations, told another government employee that she suspected that the subject was listening to her telephone calls. The other employee reported the incident.

The investigation determined that, from approximately 1998 to 2003, the employee tasked nine telephone numbers of female foreign nationals, without a valid foreign intelligence purpose, and listened to collected phone conversations while assigned to foreign locations. The subject conducted call chaining on one of the numbers and tasked the resultant numbers. He also incidentally collected the communications of a U.S. person on two occasions.

The appropriate agency referred the matter to DoJ. The subject was suspended without pay pending the outcome of the investigation and resigned before discipline had been proposed.

5. Civilian Employee, Foreign Location

The employee's agency discovered that an employee had misused the SIGINT collection system between 2001 and 2003 by targeting three female foreign nationals.

The appropriate OIG conducted an investigation. The violations were referred to DoJ. The subject resigned before disciplinary action was taken.

6. Civilian Employee, Foreign Location

As the result of a polygraph examination, it was discovered that an employee had accessed the collection of communications on two foreign nationals.

The employee's agency concluded its investigation in 2006, and the subject received a one-year letter of reprimand (prohibiting promotions, awards, and within-grade increases) and a 10 day suspension without pay. The subject's pending permanent-change-of-station assignment was cancelled, and his promotion recommendation was withdrawn.

7. Civilian Employee, Foreign Location

In 2011, the NSA OIG was notified that, in 2011, the subject had tasked the telephone number of her foreign-national boyfriend and other foreign nationals and that she reviewed the resultant collection. The subject reported this activity during an investigation into another matter.

The subject asserted that it was her practice to enter foreign national phone numbers she obtained in social settings into the SIGINT system to ensure that she was not talking to "shady characters" and to help mission.

The appropriate OIG found that the subject's actions potentially violated Executive Order 12333, Part 1.7(c)(1), and DoD Regulation 5240.1-R, Procedure 14.

The appropriate OIG referred the matter to DoJ in 2011 as a possible violation of 18 U.S.C. §2511 (interception and disclosure of electronic communications). The subject resigned before disciplinary action had been imposed.

8. Military Member, CONUS Site

In 2005, the NSA OIG was notified that, on the subject's first day of access to the SIGINT collection system, he queried six e-mail addresses belonging to a former girlfriend, a U.S. person, without authorization. A site review of SIGINT audit discovered the queries four days after they had occurred.

The subject testified that he wanted to practice on the system and had decided to use this former girlfriend's e-mail addresses. He also testified that he received no information as a result of his queries and had not read any U.S. person's e-mail.

The NSA OIG concluded that the subject's actions violated USSID 18, Executive Order 12333, 5 CFR §2635.704, and DoD Regulation 5240.1-R.

The OIG report was forwarded to the site command and the OGC. As a result of a Uniform Code of Military Justice Article 15 proceeding, the subject received a reduction in grade, 45 days restriction, 45 days of extra duty, and half pay for two months. It was recommended that the subject not be given a security clearance.

9. Civilian Employee, CONUS Site

In 2006, the Office of Oversight and Compliance within NSA's Signals Intelligence Directorate informed NSA OIG that, between 2005 and 2006, the subject had without authorization queried in two SIGINT systems the telephone numbers of two foreign nationals, one of whom was his girlfriend. On one occasion, the subject performed a text query of his own name in a SIGINT system.

The OIG investigation found that the subject queried his girlfriend's telephone number on many occasions and her name on two. He testified that he received only one "hit" from the queries on the girlfriend. Another number he queried, that of a foreign national language instructor, returned "insignificant information."

The subject claimed that he queried his name to see if anyone was discussing his travel and the telephone numbers to ensure that there were no security problems.

The OIG concluded that the subject's actions violated Executive Order 12333, 5 C.F.R. §2635.704, DoD Regulation 5240.1-R, and NSA/CSS PMM, Chapter 366 (General Principles for on the job conduct; Use of Government Resources, and Insubordination).

The Agency has been unable to locate records as to whether a referral was made to DoJ. The subject resigned from the Agency before the proposed discipline of removal had been administered.

10. Civilian Employee, CONUS Site

In 2008, the NSA OIG was notified that a SIGINT audit had discovered a possible violation of USSID 18. An investigation revealed that, while reviewing the communications of a valid intelligence target, the subject determined that the intelligence target had a relative in the U.S. The subject queried the SIGINT system for the e-mail address of the intelligence target in 2008 and used other search terms to obtain information about the target's relative.

The OIG concluded that the subject's actions violated USSID 18, Executive Order 12333, and DoD Regulation 5240.1-R.

The OIG report was forwarded to NSA's OGC. The subject received a written reprimand.

11. Military Member, Foreign Location

In 2009, the NSA OIG was notified that, in 2009, a military member assigned to a military tactical intelligence unit queried the communications of his wife, who was also a military member stationed in a foreign location. The misuse was discovered by a review of SIGINT audit logs. The investigation by his military unit substantiated the misuse.

Through a Uniform Code of Military Justice Article 15 proceeding, the member received a reduction in rank, 45 days extra duty, and half pay for two months. The member's access to classified information was revoked.

In 2009 this matter was referred to DoJ.

12. Military Member, Foreign Location

In 2009, a military unit at a foreign location notified the NSA OIG that, in 2009, a military member had queried a country's telephone numbers to aid in learning that country's language. The misuse was discovered by a review of SIGINT audit logs.

The appropriate branch of the military determined that the analyst's queries were not in support of his official duties and violated USSID 18.

The member's database access and access to classified information were suspended.

I hope that this information satisfies your request.

Sincerely,

George Ellard

Dr. George Ellard
Inspector General

cc: Sen. Patrick Leahy

Exhibit 10

DIRECTOR OF NATIONAL INTELLIGENCE
WASHINGTON, D.C. 20511

JUN 2 1 2013

The Honorable Dianne Feinstein
Chairman
Select Committee on Intelligence
United States Senate
Washington, D.C. 20510

Dear Madam Chairman:

Because of the charged rhetoric and heated controversy prompted by my response to a question Senator Ron Wyden asked me last March 12th during an unclassified threat assessment hearing before the Senate Select Committee on Intelligence, I am using this direct means of communication with you to set the record straight.

Near the end of the hearing, Senator Wyden asked the following question:

> And this is for you, Director Clapper, again on the surveillance front. And I hope we can do this in just a yes or no answer because I know Senator Feinstein wants to move on.
>
> Last summer, the NSA director was at a conference, and he was asked a question about the NSA surveillance of Americans. He replied, and I quote here, "The story that we have millions or hundreds of millions of dossiers on people is completely false."
>
> The reason I'm asking the question is, having served on the committee now for a dozen years, I don't really know what a dossier is in this context. So what I wanted to see is if you could give me a yes or no answer to the question, does the NSA collect any type of data at all on millions or hundreds of millions of Americans?

I have thought long and hard to re-create what went through my mind at the time. In light of Senator Wyden's reference to "dossiers" and faced with the challenge of trying to give an unclassified answer about our intelligence collection activities, many of which are classified, I simply didn't think of Section 215 of the Patriot Act. Instead, my answer addressed collection of the content of communications. I focused in particular on Section 702 of FISA, because we had just been through a year-long campaign to seek reauthorization of this provision and had had many classified discussions about it, including with Senator Wyden. That is why I added a comment about "inadvertent" collection of U.S. person information, because that is what happens under Section 702 even though it is targeted at foreigners.

That said, I realized later that Senator Wyden was asking about Section 215 metadata collection, rather than content collection. Thus, my response was clearly erroneous—for which I apologize. While my staff acknowledged the error to Senator Wyden's staff soon after the hearing, I can now openly correct it because the existence of the metadata collection program has been declassified.

Next month will mark for me 50 years of service to this country, virtually all of it in intelligence. In the last 20 of those years, I have appeared before Congressional hearings and briefings dozens of times, and have answered thousands of questions, either orally or in writing. I take all such appearances seriously and prepare rigorously for them. But mistakes will happen, and when I make one, I correct it.

I am sending originals of this letter to the other leaders of the intelligence oversight committees. If you have any questions regarding this matter, please contact me.

Respectfully –
Jim
James R. Clapper

Exhibit 11

United States Senate

WASHINGTON, DC 20510

June 24, 2013

General Keith Alexander
Director
National Security Agency
Fort Meade, MD 20755

Dear General Alexander:

The NSA recently released a fact sheet on surveillance authorities that contains information about both section 702 of the Foreign Intelligence Surveillance Act (FISA) and section 215 of the USA Patriot Act. As you know, section 215 of the Patriot Act is the basis for the NSA's bulk phone records collection program, while section 702 of FISA governs the collection of phone and internet communications, and involves the PRISM computer system.

We were disappointed to see that this fact sheet contains an inaccurate statement about how the section 702 authority has been interpreted by the US government. In our judgment this inaccuracy is significant, as it portrays protections for Americans' privacy as being significantly stronger than they actually are. We have identified this inaccurate statement in the classified attachment to this letter.

We urge you to correct this statement as soon as possible. As you have seen, when the NSA makes inaccurate statements about government surveillance and fails to correct the public record, it can decrease public confidence in the NSA's openness and its commitment to protecting Americans' constitutional rights. Rebuilding this confidence will require a willingness to correct misstatements and a willingness to make reforms where appropriate.

Separately, we note that this same fact sheet states that under section 702, "Any inadvertently acquired communication of or concerning a US person must be promptly destroyed if it is neither relevant to the authorized purpose nor evidence of a crime." We believe that this statement is somewhat misleading, in that it implies that the NSA has the ability to determine how many American communications it has collected under section 702, or that the law does not allow the NSA to deliberately search for the records of particular Americans. In fact, the intelligence community has told us repeatedly that it is "not reasonably possible to identify the number of people located in the United States whose communications may have been reviewed under the authority" of the FISA Amendments Act.

We appreciate your attention to this matter. We believe that the US government should have broad authorities to investigate terrorism and espionage, and that it is possible to aggressively pursue terrorists without compromising the constitutional rights of ordinary Americans. Achieving this goal depends not just on secret courts and secret congressional hearings, but on informed public debate as well. We look forward to your response.

Sincerely,

Ron Wyden

Mark Udall

Exhibit 12

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

25 June 2013

The Honorable Ron Wyden
United States Senate
221 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Mark Udall
United States Senate
328 Hart Senate Office Building
Washington, DC 20510

Dear Senators Wyden and Udall:

Thank you for your letter dated 24 June 2013. After reviewing your letter, I agree that the fact sheet that the National Security Agency posted on its website on 18 June 2013 could have more precisely described the requirements for collection under Section 702 of the FISA Amendments Act. This statute allows for "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. 1881(a). The statute provides several express limitations, namely that such acquisition:

(1) may not intentionally target any person known at the time of acquisition to be located in the United States;

(2) may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States;

(3) may not intentionally target a United States person reasonably believed to be located outside the United States;

(4) may not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States; and

(5) shall be conducted in a manner consistent with the fourth amendment to the Constitution of the United States. 50 U.S.C. 1881(b).

With respect to the second point raised in your 24 June 2013 letter, the fact sheet did not imply nor was it intended to imply "that NSA has the ability to determine how many American communications it has collected under section 702, or that the law does not allow the NSA to deliberately search for the records of particular Americans." As you correctly state, this point has been addressed publicly. I refer you to unclassified correspondence from the Director of National Intelligence dated 26 July 2012 and 24 August 2012.

NSA continues to support the effort led by the Office of the Director of National Intelligence and the Department of Justice to make publicly available as much information as possible about recently disclosed intelligence programs, consistent with the need to protect national security and sensitive sources and methods.

KEITH B. ALEXANDER
General, U.S. Army
Director, NSA/Chief, CSS

Copies Furnished:

The Honorable Dianne Feinstein
Chairman, Select Committee on Intelligence

The Honorable Saxby Chambliss
Vice Chairman, Select Committee on Intelligence

Exhibit 13

Section 702

Title VII, Section 702 of the Foreign Intelligence Surveillance Act (FISA), "Procedures for Targeting Certain Persons Outside the United States Other Than United States Persons" (50 U.S.C. sec. 1881a)

- This authority allows only the targeting, for foreign intelligence purposes, of communications of foreign persons who are located abroad.

- The government may not target any U.S. person anywhere in the world under this authority, nor may it target a person outside of the U.S. if the purpose is to acquire information from a particular, known person inside the U.S.

- Under this authority, the Foreign Intelligence Surveillance Court annually reviews "certifications" jointly submitted by the U.S. Attorney General and Director of National Intelligence.

- These certifications define the categories of foreign actors that may be appropriately targeted, and by law, must include specific targeting and minimization procedures adopted by the Attorney General in consultation with the Director of National Intelligence and approved by the Court as consistent with the law and 4th Amendment to the Constitution.

- There must be a valid, documented foreign intelligence purpose, such as counterterrorism, for each use of this authority. All targeting decisions must be documented in advance.

- The Department of Justice and the Office of the Director of National Intelligence conduct on-site reviews of targeting, minimization, and dissemination decisions at least every 60 days.

- The Foreign Intelligence Surveillance Court must approve the targeting and minimization procedures, which helps ensure the protection of privacy and civil liberties.

- These procedures require that the acquisition of information is conducted, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized foreign intelligence purpose.

- Any inadvertently acquired communication of or concerning a U.S. person must be promptly destroyed if it is neither relevant to the authorized purpose nor evidence of a crime.

- If a target who was reasonably believed to be a non-U.S. person outside of the U.S. either enters the U.S. or was in fact a U.S. person at the time of acquisition, targeting must be immediately terminated.

- Any information collected after a foreign target enters the U.S. –or prior to a discovery that any target erroneously believed to be foreign was in fact a U.S. person– must be promptly destroyed unless that information meets specific, limited criteria approved by the Foreign Intelligence Surveillance Court.

- The dissemination of any information about U.S. persons is expressly prohibited unless it is necessary to understand foreign intelligence or assess its importance; is evidence of a crime; or indicates a threat of death or serious bodily harm.

- The FISC rules of procedure require immediate reporting of any compliance incident. In addition, the government reports quarterly to the FISC regarding any compliance issues that have arisen during the reporting period, including updates of previously reported incidents.

- The Department of Justice and Office of the Director of National Intelligence provide a semi-annual assessment to the Court and Congress assessing compliance with the targeting and minimization procedures. In addition, the Department of Justice provides semi-annual reports to the Court and Congress concerning implementation of Section 702.

- An annual Inspector General assessment is provided to Congress, reporting on compliance with procedural requirements, the number of disseminations relating to U.S. persons, and the number of targets later found to be located inside the U.S.

Section 215

Section 215 of the USA PATRIOT Act of 2001, which amended Title V, Section 501 of the Foreign Intelligence Surveillance Act (FISA), "Access to Certain Business Records for Foreign Intelligence and International Terrorism Investigations" (50 U.S.C. sec. 1861)

- This program concerns the collection only of telephone metadata. Under this program, the government does not acquire the content of any communication, the identity of any party to the communication, or any cell-site locational information.

- This metadata is stored in repositories within secure networks, must be uniquely marked, and can only be accessed by a limited number of authorized personnel who have received appropriate and adequate training.

- This metadata may be queried only when there is a reasonable suspicion, based on specific and articulated facts, that the identifier that will be used as the basis for the query is associated with specific foreign terrorist organizations.

- The basis for these queries must be documented in writing in advance.

- Fewer than two dozen NSA officials may approve such queries.

- The documented basis for these queries is regularly audited by the Department of Justice.

- Only seven senior officials may authorize the dissemination of any U.S. person information outside of NSA (e.g. to the FBI) after determining that the information is related to and is necessary to understand counterterrorism information, or assess its importance.

- Every 30 days, the government must file with the Foreign Intelligence Surveillance Court a report describing the implementation of the program, to include a discussion of the application of the Reasonable Articulable Suspicion (RAS) standard, the number of approved queries and the number of instances that query results that contain U.S. person information were shared outside of NSA in any form.

- The Foreign Intelligence Surveillance Court reviews and must reauthorize the program every 90 days.

- At least once every 90 days, DOJ must meet with the NSA Office of Inspector General to discuss their respective oversight responsibilities and assess NSA's compliance with the Court's orders.

- At least once every 90 days, representatives from DOJ, ODNI and NSA meet to assess compliance with the Court's orders.

- Metadata collected under this program that has not been reviewed and minimized must be destroyed within 5 years.

- DOJ and NSA must consult on all significant legal opinions that relate to the interpretation, scope, and/or implementation of this authority.

Exhibit 14

F. JAMES SENSENBRENNER, JR.
FIFTH DISTRICT, WISCONSIN

COMMITTEE ON THE JUDICIARY

SUBCOMMITTEE ON
CRIME, TERRORISM, AND
HOMELAND SECURITY
CHAIRMAN

COMMITTEE ON SCIENCE, SPACE,
AND TECHNOLOGY
VICE-CHAIRMAN

Congress of the United States
House of Representatives
Washington, DC 20515–4905

WASHINGTON OFFICE:
ROOM 2449
RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–4905
202–225–5101

DISTRICT OFFICE:
120 BISHOPS WAY, ROOM 154
BROOKFIELD, WI 53005–6294
262–784–1111

OUTSIDE MILWAUKEE METRO
CALLING AREA:
1–800–242–1119

WEBSITE:
HTTP://SENSENBRENNER.HOUSE.GOV

September 6, 2013

The Honorable Eric H. Holder, Jr.
Attorney General
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, D.C. 20530

Dear Attorney General Holder:

The administration's legal interpretation of Section 215 of the Patriot Act—until recently secret—has been the subject of intense criticism since details of the National Security Agency's bulk collection of phone data became public. Section 215 allows the government to apply to the Foreign Intelligence Surveillance Court to issue an order for the production of tangible things if they are relevant to an authorized investigation into international terrorism.[1]

Under this relevance standard, the administration has collected the details of every call made by every American, even though the overwhelming majority of these calls have nothing to do with terrorism. In passing Section 215, Congress intended to allow the government access to *specific* records. The administration's interpretation to allow for bulk collection is at odds with Congressional intent and with both the plain and legal meanings of "relevance."[2]

The implications of this flawed interpretation are staggering. The logic the administration uses for bulk collection would seem to support bulk collection of other personal data. A Federal Bureau of Investigation's (FBI) training manual specifically lists library records, book sales, firearm sales, tax returns, educational records, and medical records as examples of records the administration can obtain under the Patriot Act.[3] The breadth of the administration's argument raises the question: What other records does the administration believe it can collect in bulk pertaining to every American?

In defending its bulk collection of phone records, the administration explicitly stated that its "conclusion does *not* mean that any and all types of business records—such as medical records or library or bookstore records—could be collected in bulk under this authority."[4] Phone records are apparently

---

1 50 U.S.C. § 1861.

2 Rep. Jim Sensenbrenner, *How Obama has Abused the Patriot Act*, L.A. Times (August 19, 2013).

3 FBI Training Manual on Foreign Intelligence Surveillance Act.

4 Administration White Paper: Bulk Collection of Telephony Metadata under Section 215 of the USA Patriot Act (August 9, 2013).

different from medical, library, and bookstore records because of the importance of the connections between individual data points.[5]

While it is unclear how the interconnectedness of data heightens the relevance of communications even where none of the communications are relevant, it is significant that this interconnectedness is not unique to phone records. Any commercial transaction involves interaction between multiple parties.

In, for example, a firearms sale, the FBI could easily conclude that it is interested, not only in the type of firearms being purchased, but also in who is selling firearms to whom—thereby ascribing importance to the connection between the buyers and sellers. The potential importance of these connections makes commercial transactions like firearms sales indistinguishable from phone records under the administration's analysis. The administration's sweeping legal view of Section 215 could support building a national gun registry despite Congress's express disapproval and the Second Amendment.

While this further highlights the flaws in the administration's interpretation of Section 215, it also raises important privacy questions. Please respond to the following by September 30, 2013:

1. Does the Department of Justice (Department) believe Section 215 of the Patriot Act authorizes it to collect all records of commercial transaction between Americans?
2. Does the Department believe that it has the authority to bulk collect all records of firearms sales?
3. Does the Department believe that Section 215 allows the administration to assemble a database of gun owners?
4. Is the administration collecting records in bulk other than phone records?
5. If the Department does not believe it has the authority to collect records of commercial transactions in bulk, how does the Department distinguish phone records from commercial transactions?

Thank you for your prompt response to this serious matter.

Sincerely,

F. JAMES SENSENBRENNER JR.
Member of Congress

---

5 *Id.* at 5.