

IN UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

LARRY KLAYMAN, *et. al*

Plaintiffs,

v.

BARACK HUSSEIN OBAMA II, *et. al*

Defendants.

Civil Action Nos. 13-cv- 851
13-cv-881

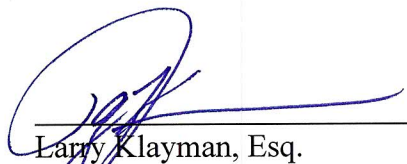
NOTICE TO APPEAR AT ORAL ARGUMENTS

TO DEFENDANT NATIONAL SECURITY AGENCY AND ITS ATTORNEY OF RECORD:

NOTICE IS HEREBY GIVEN that the records custodian or another qualified employee of the Defendant National Security Agency is hereby required to appear at the oral arguments scheduled to take place on November 18, 2013 at 11:30 a.m., in the U.S. District Court for the District of Columbia, Courtroom 18, located at 333 Constitution Ave, NW, Washington, D.C. 20001 to authenticate the documents set forth in the attached *Touhy* letter to the NSA of November 13, 2013.

Dated: November 13, 2013

Respectfully submitted,



Larry Klayman, Esq.
Attorney at Law
D.C. Bar No. 334581
2020 Pennsylvania Ave. NW, Suite 800
Washington, DC 20006

Tel: (310) 595-0800

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that on this 13th day of November, 2013 a true and correct copy of the foregoing Notice to Appear for Oral Argument (Civil Action Nos. 13-cv- 851 and 13-cv-881) was served via U.S. Mail and E-mail upon the following:

James R. Whitman
U.S. DEPARTMENT OF JUSTICE
P.O. Box 7146
Washington, DC 20044
(202) 616-4169
Fax: 202-616-4314
Email: james.whitman@usdoj.gov

James J. Gilligan
Special Litigation Counsel
Civil Division, Federal Programs Branch
U.S. Department of Justice
P.O. Box 883
Washington, D.C. 20044
(202) 514-3358
Email: James.Gilligan@usdoj.gov

Attorneys for Defendants.

Respectfully submitted,



Larry Klayman, Esq.
D.C. Bar No. 334581
Klayman Law Firm
2020 Pennsylvania Ave. NW, Suite 345
Washington, DC 20006
Tel: (310) 595-0800



November 13, 2013

URGENT

Via U.S. Mail and Email

TOUHY REQUEST FOR DOCUMENTS AND EMPLOYEE TESTIMONY

Office Of General Counsel
National Security Agency
9800 Savage Road
Ft. George G. Meade, MD 20755

James J. Gilligan, Esq.
U.S. DEPARTMENT OF JUSTICE
CIVIL DIVISION, FEDERAL PROGRAMS BRANCH
20 Massachusetts Avenue, NW
Room 5138
Washington, DC 20001

Re: Klayman v. Obama, et al. (Nos. 13-cv-851, 13-cv-881, D.C. District Court) -- Hearing of November 18, 2013, at 11:30 a.m.

Ladies and Gentlemen:

Pursuant to the request of the undersigned, Larry Klayman, this letter serves as a "Touhy Request," requesting the documents and testimony of a National Security Agency employee. *See Touhy v. Ragen*, 340 U.S. 462 (1951). This request is being sent with the enclosed notice to appear at a hearing that is being sent with regard to the above styled case. A hearing is being held on Monday, November 18, 2013, at 11:30 a.m. in Courtroom 18 of the U.S. District Court for the District of Columbia, located at 333 Constitution Ave, NW, Washington, D.C. 20001. A notice to appear is attached and enclosed.

Background.

On April 25, 2013, the Honorable Roger Vinson, a judge of the U.S. Foreign Intelligence Surveillance Court ("FISC"), issued a top-secret order compelling the disclosure of all call detail records in possession of Verizon Telecommunication for analysis by the National Security Agency ("NSA") on an ***ongoing daily basis***.¹ On June 5, 2013, based on the disclosures of whistleblower, Edward Snowden, who fled the United States for fear of government reprisal, *The*

¹ *See, In re Application of the FBI for an Order Requiring the Production of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs., Inc. d/b/a Verizon Bus. Servs.*, No. BR 13-80 (FISA Ct. Apr. 25, 2013) ("Verizon Order").

Guardian publicly revealed this previously classified order in an article entitled “NSA collecting phone records of millions of Verizon customers daily. Exclusive: Top secret order requiring Verizon to hand over all call data shows scale of domestic surveillance under Obama.”²

Prior to this disclosure, the American people had no reasonable opportunity to discover the existence of this surveillance program or its clear violation of statutory and constitutional protections.

Based on the disclosures of whistleblower Edward Snowden in *The Guardian*, the Verizon Order showed, for the first time, that the communication records of U.S. citizens are being collected indiscriminately and in bulk—regardless of whether there is reasonable suspicion or any “probable cause” of any wrongdoing.

On June 9, 2013, the undersigned filed suit challenging the legality of the government's secret and illicit government scheme to systematically gather, intercept and analyze vast quantities of domestic telephonic communications and “metadata” wholly within the United States by implementing a highly classified, unlawful mass call tracking surveillance program run by the NSA. The federal government and the NSA have far exceeded their statutory authority and, as such, violated the First, Fourth, and Fifth Amendments of the U.S. Constitution in addition to Section 215 of the Patriot Act, which is the basis of the subject lawsuit.

The information requested below is required by the undersigned and the other plaintiffs in order to determine the full scope of the Constitutional violations that have been occurring as a result of the NSA's illegal data collection programs.

Requested Testimony.

- 1) A custodian of records is required to authenticate internal memorandum and other such correspondence between the NSA and outside agencies, members of Congress, and any other documents in possession of the plaintiffs, including but not limited to the following:
 - a) United States Government Memorandum of 3 May 2012 (OC-034-12)
 - b) Memorandum for Staff Director, House Permanent Select Committee on Intelligence of 25 February 2009 (GC/009/09)
 - c) FAA Certification Renewals With Caveats on 2011-10-12 0850
 - d) Correspondence of NSA director Keith B. Alexander to Senators Ron Wyden and Mark Udall on 25 June 2013
 - e) Correspondence of Senator Chuck Grassley to Dr. George Ellard, Inspector General of the National Security Agency of August 27, 2013

² In the days after *The Guardian* disclosed the Verizon Order, the Director of National Intelligence, James Clapper, acknowledged its authenticity and issued a statement indicating that the FISC had renewed it. See Office of the Dir. Of Nat'l Intelligence, *DNI Statement on Recent Unauthorized Disclosure of Classified Information* (June 6, 2013), <http://1.usa.gov/13jwuFc>. See also, Office of the Dir. Of Nat'l Intelligence, *Foreign Intelligence Surveillance Court Renews Authority to Collect Telephony Metadata* (July 19, 2013), <http://1.usa.gov/12ThY1T>.

- f) Correspondence of Dr. George Ellard, Inspector General of the National Security Agency to Senator Chuck Grassley on 11 September 2013
- g) Powerpoint slides of PRISM/US-984XN Overview

These documents are attached to and enclosed with this letter.

- 2) Testimony by a person or persons within the NSA who are familiar with the telephony and metadata collection performed by the NSA on the American people, including but not limited to data collected by a collaboration with Verizon Communications and all other telephone and/or internet companies such as Skype, Google, Youtube, AOL, YAHOO!, Facebook, Paltalk, AT&T, Sprint, and Microsoft.

This Testimony is Not Available From Another Source.

This testimony and the subject documents are only in the possession of the NSA and only the NSA will be able to authenticate the documents obtained by the undersigned. In addition, only the NSA knows the nature and full extent of the surveillance that is being performed and will be the only ones capable of testifying about it.

Production is Appropriate in Light of Any Relevant Privilege.

There are no relevant privileges. The NSA has been secretly, and in violation of the Patriot Act and the U.S. Constitution, been performing surveillance on the American people without any probable cause or reasonable suspicion. Neither the government nor the NSA can present any relevant privilege that will allow them to act in clear violation of the law.

Production Is Appropriate Under The Applicable Rules Of Discovery Or The Procedures Governing The Case Or Matter In Which The Demand Arose.

The Federal Rules of Civil Procedure and Evidence apply since the presiding jurisdiction is the U.S. District Court for the District of Columbia. Under the Federal Rules of Evidence, Rule 401, evidence is relevant if: (a) it has any tendency to make a fact more or less probable than it would be without the evidence; and (b) the fact is of consequence in determining the action.

Any evidence of the extent of the NSA's surveillance is directly relevant to the claims and allegations made by the undersigned and the other plaintiffs in the above styled lawsuit. The method and amount of data collected by the NSA is of direct consequence to whether they are acting in violation the Patriot Act and the U.S. Constitution.

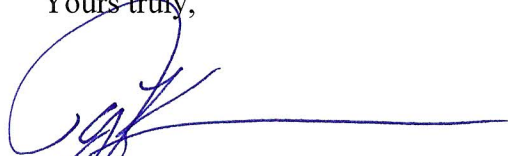
Disclosure Would Not Violate Any Statutes, Responsibilities, Regulations, or Directives of the NSA, Nor Would it Reveal Classified Information.

The undersigned seeks to verify the authenticity of information that has already been release to the American people. The disclosure of such information has already been made, and the authentication is only required for the legal proceedings.

Description of Testimony Sought.

As described above, the undersigned seeks the testimony of a custodian of records who can authenticate the documents currently in his possession. In addition, the undersigned is requesting an employee or employees who can describe the method and amount of telephony and metadata that is collected by the NSA.

Yours truly,

A handwritten signature in blue ink, appearing to be 'L. Klayman', with a long horizontal line extending to the right.

Larry Klayman

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) NSA SID-reported Incidents by Authority

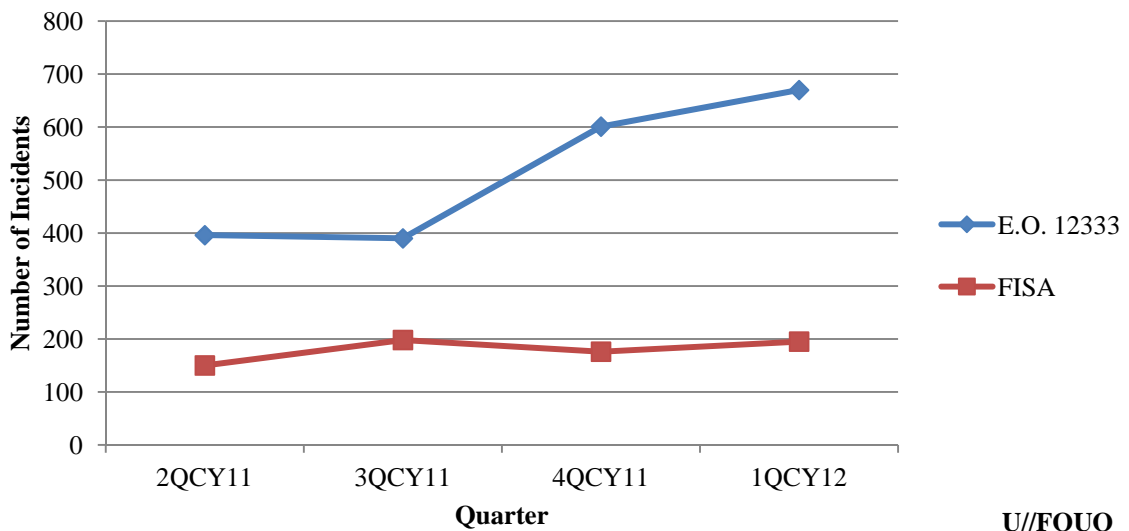
(TS//SI//REL TO USA, FVEY) **Figures 1a-b** compares all categories of NSA SID-reported incidents (collection, dissemination, unauthorized access, and retention) by Authority for 2QCY11 – 1QCY12. From 4QCY11 to 1QCY12, there was an overall increase in incidents of 11%. There was also an increase of 11% 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) roamer¹ 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 NSA 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 NSA SID-reported Incidents by Authority
U//FOUO



(U//FOUO)

(TS//SI//NF) **FISA Incidents:** As reflected in **Figures 1a-b**, during 1QCY12, NSA SID reported a total of 195 FISA incidents, 185 of which were associated with unintentional collection. NSA 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).

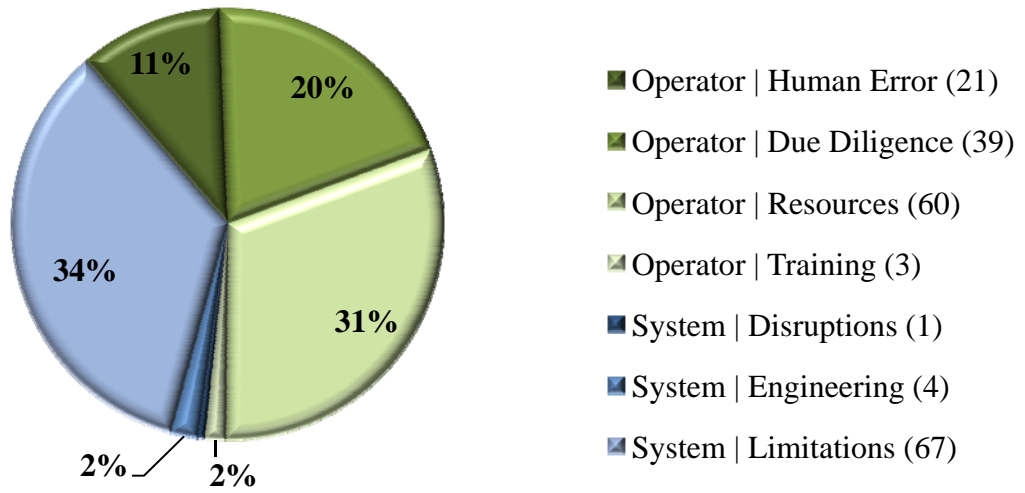
(U//FOUO) The Resources root cause category accounted for the largest percentage of Operator Error incidents under FISA authorities for 1QCY12. Analysis identified that these incidents could be reduced if analysts had more complete and consistent information available about selectors and/or targets at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



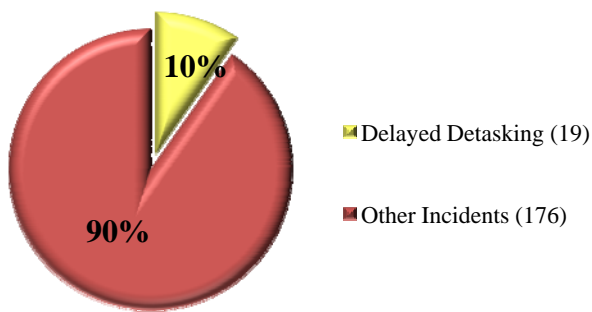
Total: 195

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**

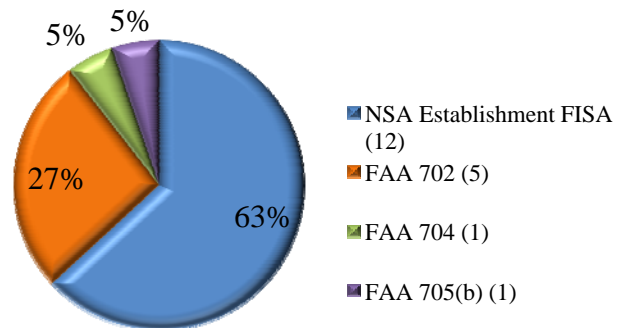
U//FOUO



Total: 195

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

U//FOUO



Total: 19

U//FOUO

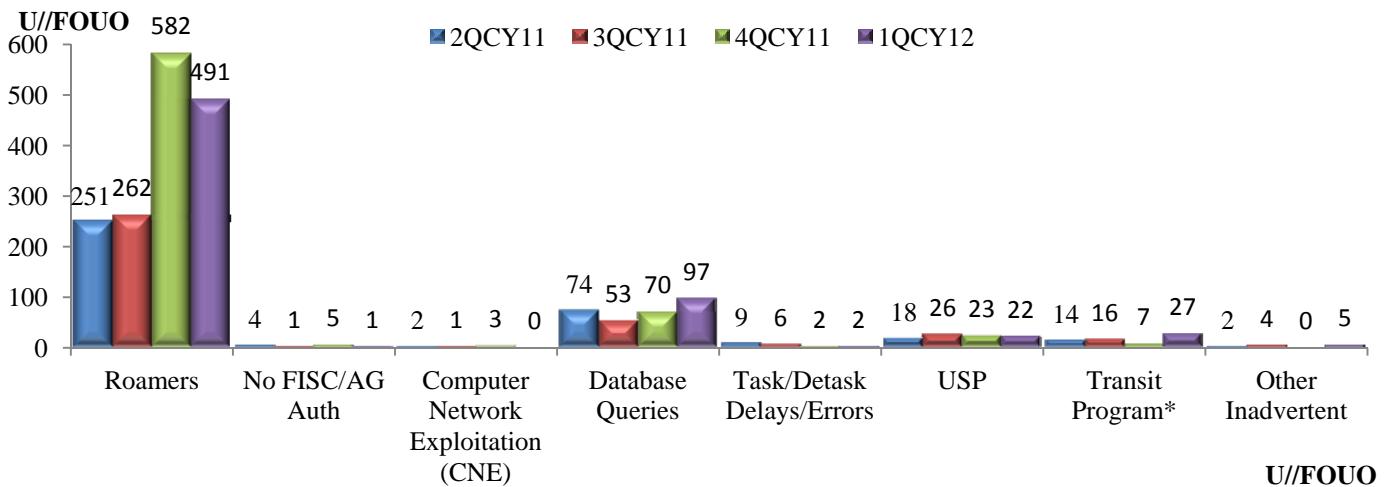
U//FOUO

(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. NSA SID-reported Collection Incidents by Sub-Type and Authority

(U//FOUO) **Figures 4a-b** depicts NSA 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.

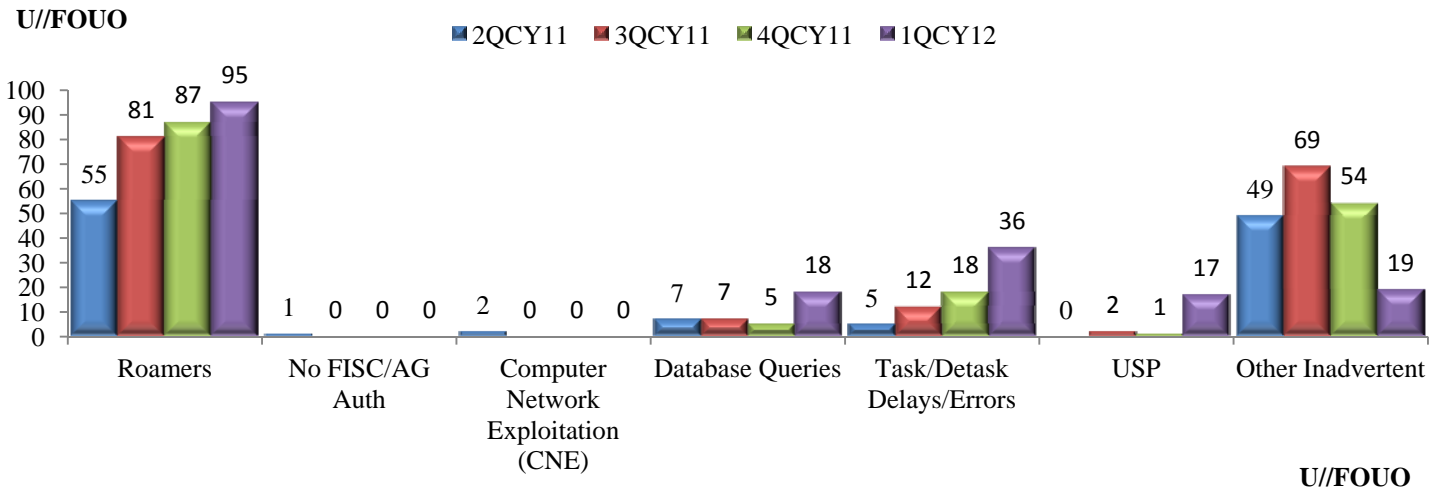
(U//FOUO) **Figure 4a:** NSA SID-reported Collection Incidents Under E.O. 12333 Authority



(U//FOUO) **Figure 4a:** During 1QCY12, NSA 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).

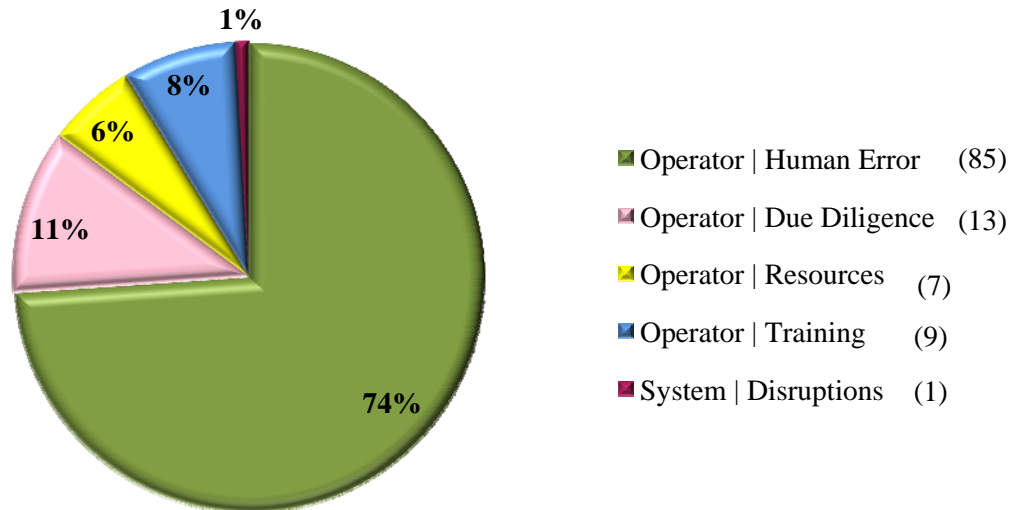
(U//FOUO) The remaining 1 database query incident can be attributed to System Error as the root cause and occurred due to a mechanical error with the tool.

(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

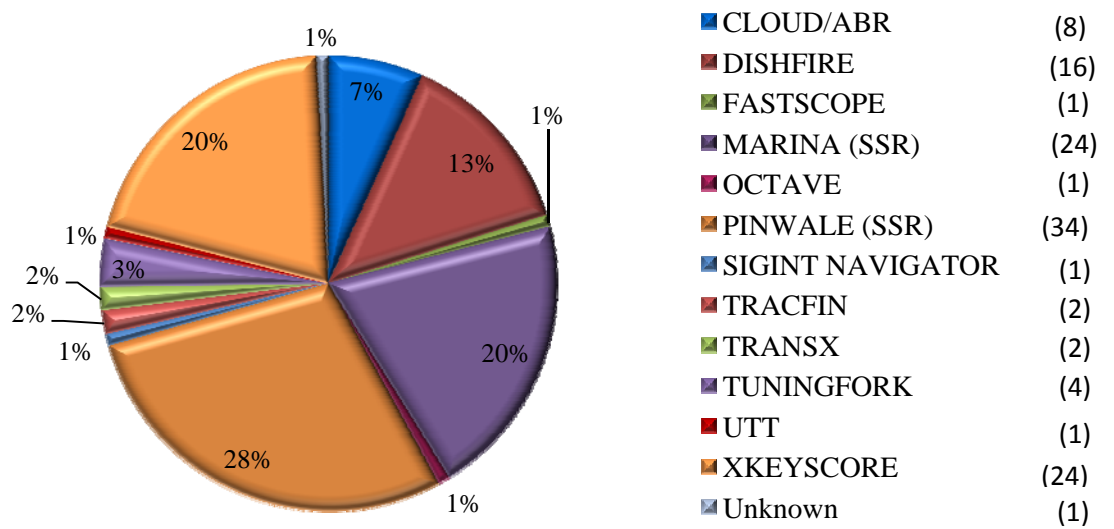
U//FOUO

(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



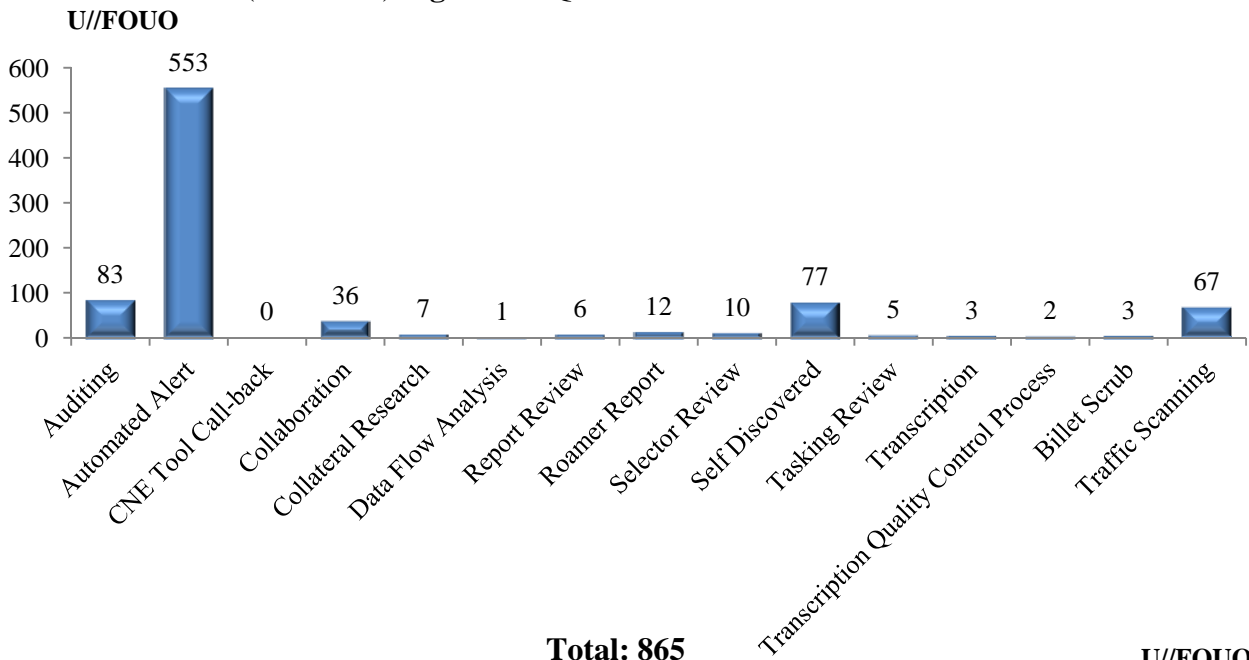
Total: 119

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**



Total: 865

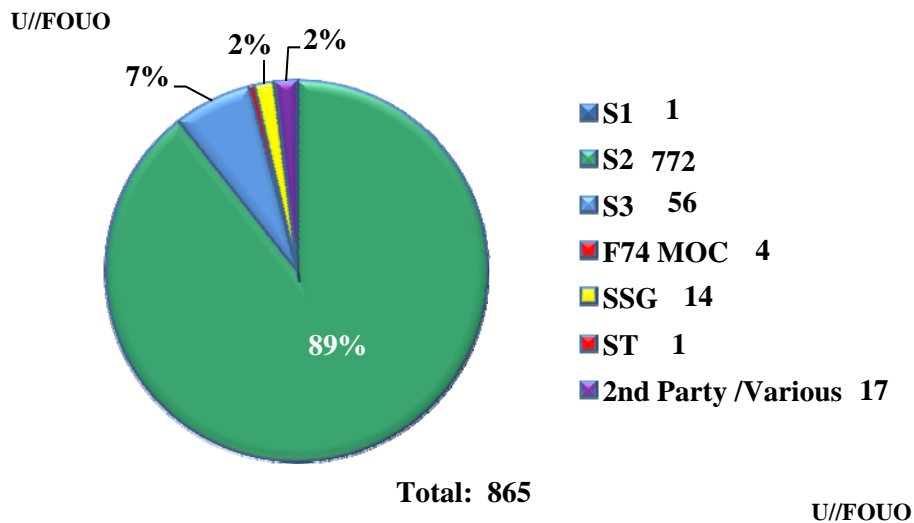
U//FOUO

(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) NSA SID-reported Incidents by Organization

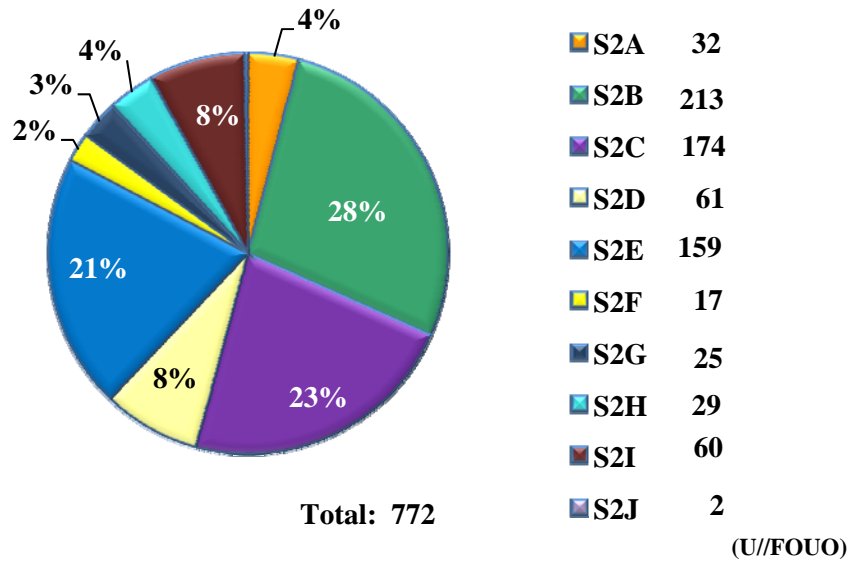
(U//FOUO) **Figure 8** illustrates the total 1QCY12 NSA SID-reported incidents by primary SID Deputy Directorate (DD) level organization. S2, having the largest NSA SID contingent of reported incidents, accounted for 89% of the total incidents for the quarter, a proportion consistent with the overall 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 NSA SID Organization



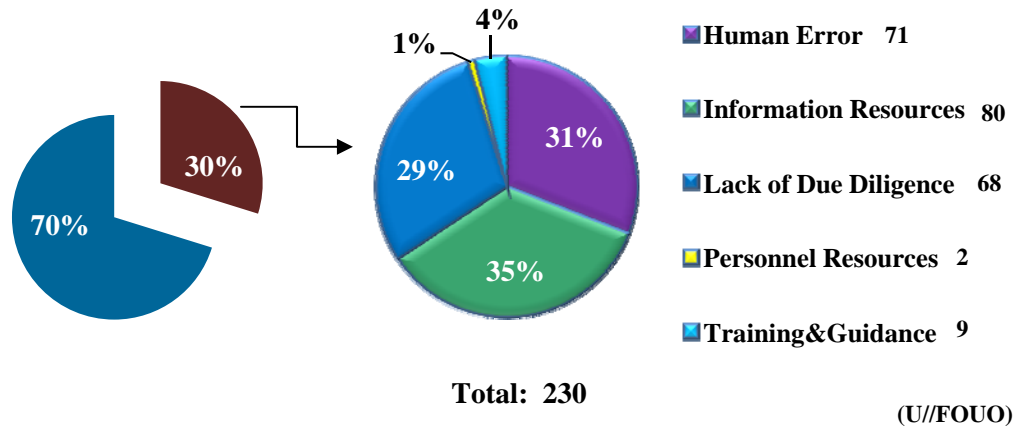
(U//FOUO) **Figure 9** provides a look into S2 (by Product Line) as the NSA SID organization with the largest number of reported incidents. For 1QCY12, three Product Lines accounted for 72% of S2's reported incidents. These Product Lines were: the and Korea Division (S2B) with 28% of the reported incidents, 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) **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)



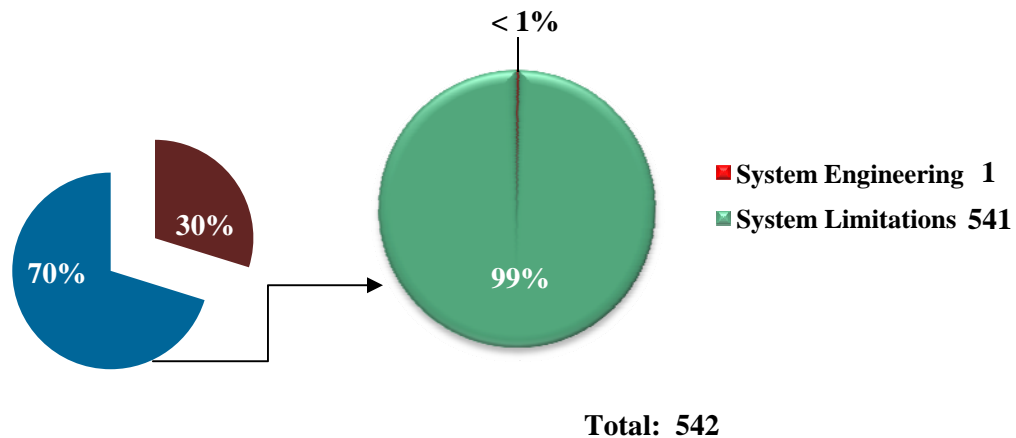
(U//FOUO) 30% of the S2-reported incidents during 1QCY12 are attributed to Operator Error as the root cause, and involved:

- 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)



(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 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 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 2011 [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 Qureshi 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 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.


Chief, SID Oversight & Compliance

All redacted
information exempt
under (b)(1) and (b)(3)
except as otherwise
noted.



~~TOP SECRET//COMINT//NOFORN~~
NATIONAL SECURITY AGENCY

FORT GEORGE G. MEADE, MARYLAND 20755-6000

Serial: GC/009/09
25 February 2009

MEMORANDUM FOR STAFF DIRECTOR, HOUSE PERMANENT SELECT
COMMITTEE ON INTELLIGENCE

SUBJECT: (U) Congressional Notification - Incidents of Noncompliance -
INFORMATION MEMORANDUM

(U) The purpose of this correspondence is to notify the Committee of compliance matters that are currently under review by the Foreign Intelligence Surveillance Court and which relate to subjects of prior testimony to the Congress.

~~(TS//SI//NF)~~ Under two separate sets of orders issued by the Court pursuant to Sections 1841 and 1861 of the Foreign Intelligence Surveillance Act of 1978, as amended ("FISA"), the National Security Agency ("NSA" or "Agency") receives telephony and electronic communications metadata in order to produce foreign intelligence related to the activities of [REDACTED] the [REDACTED]

On 15 January 2009, the Department of Justice ("DoJ") notified the Court that an automated alert process NSA used to compare the telephony metadata against a list of telephone identifiers that were of foreign intelligence interest to NSA's counterterrorism personnel did not operate in conformity with the Court's orders. The Government also advised the Court that NSA had incorrectly described the alert process in prior reports to the Court. As part of a comprehensive review ordered by the Director of NSA, the Agency identified another automated process used to query the telephony metadata that also did not operate in conformity with the Court's orders. The review also identified some manually entered queries that were noncompliant with the Court's orders. None of the compliance incidents resulted in the dissemination of any reporting from NSA to any other department or agency. Upon discovery of these compliance incidents, NSA immediately made changes to its processes to ensure that the Agency is handling and querying the telephony metadata in accordance with the Court's orders. The corrective measures include implementation of controls that prevent any automated process from querying the telephony metadata NSA receives pursuant to the Court's orders and which also guard against manual querying errors.

Derived From: NSA/CSSM 1-52

Dated: 20070108

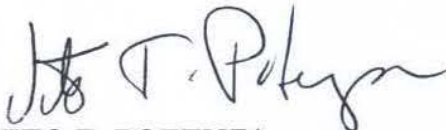
Declassify On: ~~20320108~~

~~TOP SECRET//COMINT//NOFORN~~

~~(TS//SI//NF)~~ In response to the Government's compliance notice, on 28 January 2009, the Court directed the Government to file a brief and supporting documentation describing how the compliance and misreporting incidents occurred so the Court can determine what remedial action, if any, is warranted. Since the Court was aware that there are similarities between NSA's processing of telephony metadata and electronic communications metadata under separate orders, the Court also directed the Government to determine whether NSA has been processing the electronic communications metadata in accordance with the terms of the Court's orders for this category of material. As part of this review, the Government concluded that NSA was processing the electronic communications metadata in accordance with the terms of the Court's orders, with one exception. The review identified one particular process that the Government concluded was not in conformity with the Court's order. NSA had employed the process in a small number of cases to approve queries against the electronic communications metadata. Although the Agency had previously reported the process to the Court [REDACTED] [REDACTED] this process, too, has been discontinued.

~~(S)~~ NSA and DoJ have already identified a number of steps designed to improve the Agency's ability to comply with the relevant orders and implementation of these changes has begun. Also, in addition to notifying the Court, the Government has notified a number of senior Executive Branch officials about these compliance matters. Officials who have received such notification include the President's Intelligence Oversight Board, the Director of National Intelligence, NSA's Inspector General, and the Under Secretary of Defense for Intelligence. My office is also prepared to brief the Committee on these matters at the Committee's convenience.

(U) Should you have any questions, please contact Jonathan E. Miller, Associate Director of Legislative Affairs, at [REDACTED]



VITO T. POTENZA
General Counsel

Copy Furnished:
Minority Staff Director, House Permanent
Select Committee on Intelligence



(TS//SI//NF) FAA Certification Renewals With Caveats
By [REDACTED] on 2011-10-12 0850

(TS//SI//NF) The FISA Court signed the 2011 FAA Certifications on 3 Oct 2011 – these are valid until 2 Oct 2012, permitting SSO FAA-authorized accesses to continue operations. However, in the 80-page opinion, the judge ordered certain “upstream” or “passive” FAA DNI collection to cease after 30 days, unless NSA implements solutions to correct all deficiencies identified in the opinion document. PRISM operations are not affected by these caveats. All PRISM providers, except Yahoo and Google, were successfully transitioned to the new Certifications. We expect Yahoo and Google to complete transitioning by Friday 6 Oct. Regarding the non-PRISM FAA collection programs, the Court cited targeting and minimization procedures related to collection of Multiple Communications Transactions as “deficient on statutory and constitutional grounds.” SSO, Technology Directorate, OGC, and other organizations are coordinating a response, which includes planning to implement a conservative solution in which the higher-risk collection will be sequestered. It is possible that this higher risk collection contains much of the non-duplicative FAA collection resulting in FAA reporting from upstream accesses. This solution is designed to comply with the judge’s order; however, the judge will have to determine if it does. If the solution is installed, SSO will then work with OPIs and OGC to modify the solution over time such that the filtering process will be optimized to permit more valid collection to be processed and forwarded to OPIs. Finally, in parallel with these efforts, the OGC is contemplating filing an appeal to the ruling.



NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-8000

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

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

© 2008, Senator Grassley

UNCLASSIFIED



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.

UNCLASSIFIED

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.

UNCLASSIFIED

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.

UNCLASSIFIED

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.

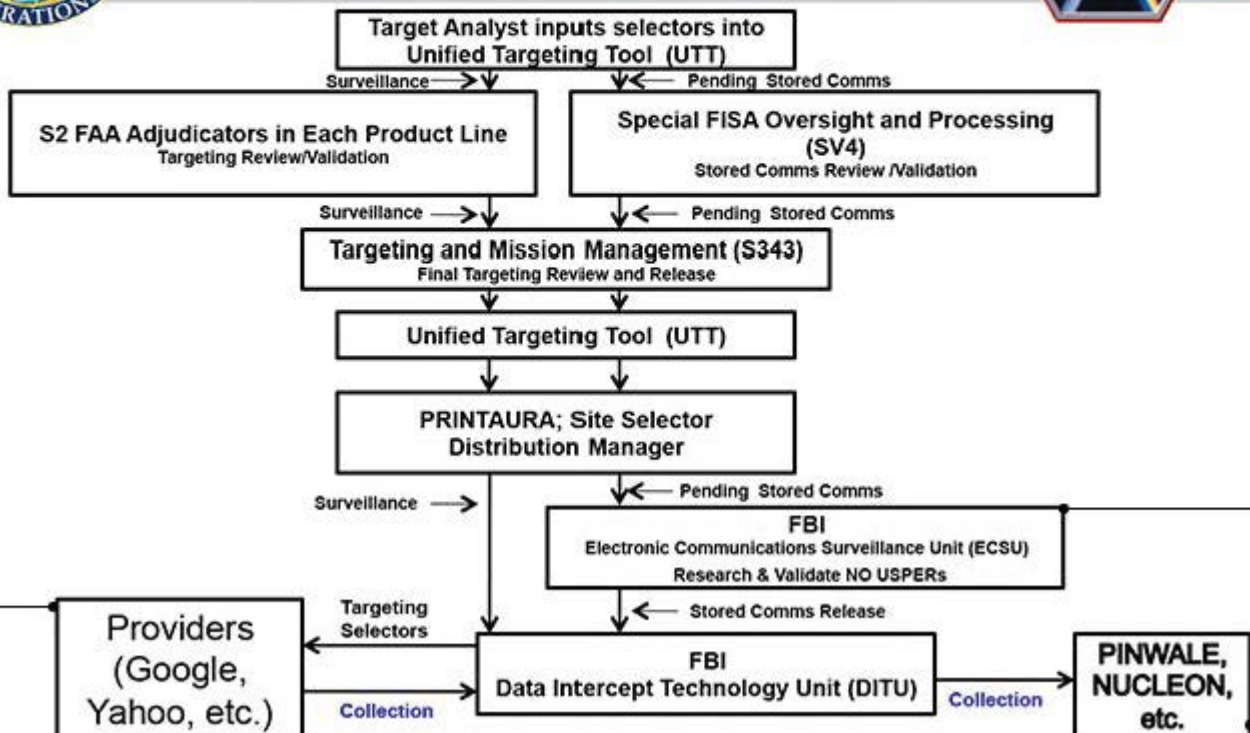
Sincerely,


Dr. George Ellard
Inspector General

cc: Sen. Patrick Leahy

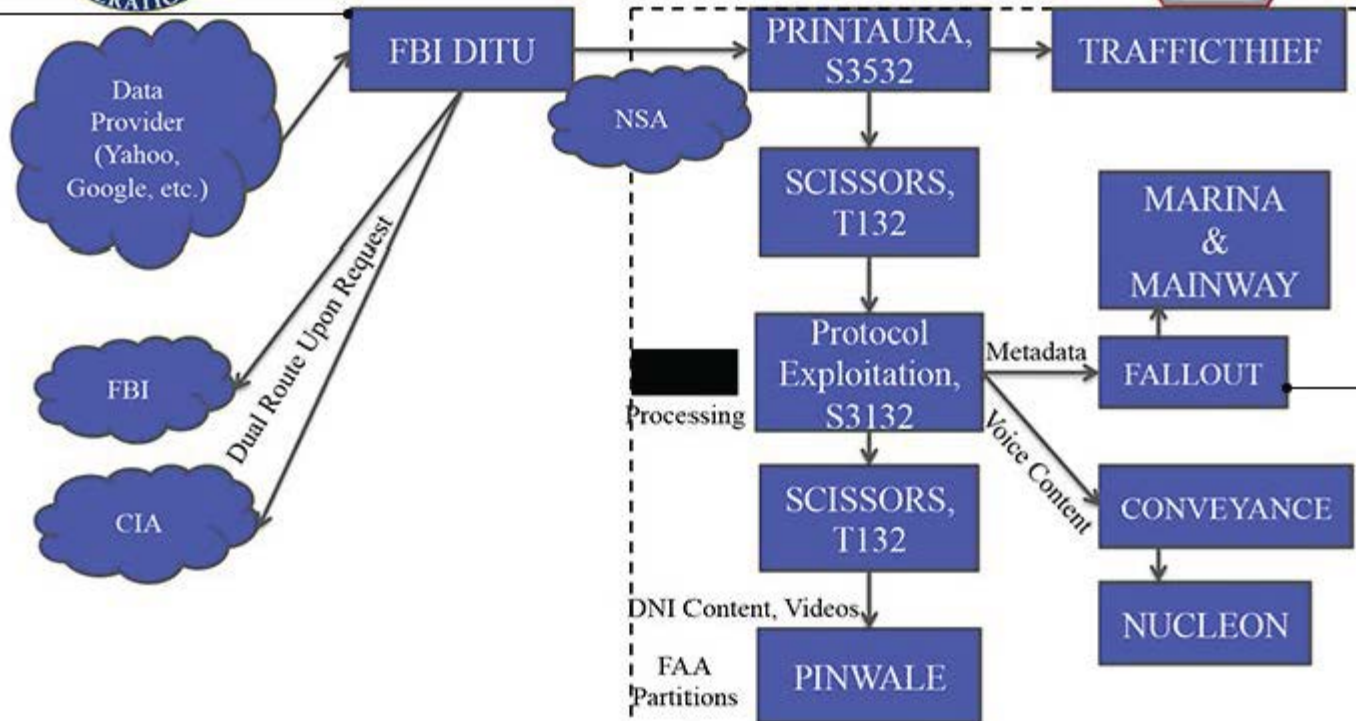


(TS//SI//NF) PRISM Tasking Process





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





facebook



Hotmail

YAHOO!



YouTube

AOL mail



(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



facebook



Hotmail



AOL mail



(TS//SI//NF) REPRISMFISA TIPS

(https:// [REDACTED])



DYNAMIC PAGE - HIGHEST POSSIBLE CLASSIFICATION IS TOP SECRET//SI,TK//ORCON,NOFORN

REPRISMFISA

COUNTERTERRORISM

[REDACTED] 2013-Apr-05 10:10:28Z

Click on the PRISM icon first
(from the initial webpage)



PRISM ENTRIES

Last Lead on Apr 05, 2013 at 12:22 PM GMT

Check the total record status, click on this link

QUICK LINKS

- See Entry List (Current)
- See Entry List (Expired)
- See Entry List (Current and Expired)
- See NSA List
- See New Records
- Ownership Count

If the total count is much less than this,
REPRISMFISA is having issues, E-MAIL
the REPRISMFISA HELP DESK AT

AND INFORM THEM

Records: 1 - 58 out of 187875 Page: 1 of 254 Records per page: 50

Clear Sort Order Click on column headers to sort. * columns is not sortable.

SEARCH

The search form below can be used as a filter to see a partial list of records.

Search For:

 AND OR

Expiration days

(+/- from now)

Filter

Prism Current Entries