All withheld information exempt under (b)(1) and (b)(3) unless otherwise noted.
Approved for Public Release

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

U.S. FOREIGN INTELLIGENCE SURVEILLANCE COURT
2015 OCT 21 PM 4:54
LEEANN FLYNN HALL
CLERK OF COURT

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

[redacted]

(U) GOVERNMENT'S VERIFIED RESPONSE TO THE COURT'S ORDER DATED OCTOBER 14, 2015

~~(TS//SI//NF)~~ The Government submits this verified response to the Order of the Foreign Intelligence Surveillance Court (FISC) issued on October 14, 2015 (hereinafter "Order"). The Order directs the Government to file a written submission regarding the Government's justification under both NSA's Section 702 Standard Minimization Procedures (SMPs) and 50 U.S.C. § 1809(a)(2) for retaining data otherwise subject to purge in two mission management systems [redacted] and [redacted].

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

~~Classified by: Chief, Oversight Section, OI, NSD, DOJ~~
~~Derived from: NSA/CSSM 1-52~~
~~Declassify on: 204010XX~~

OI Tracking No: 130611

(U) **Background**

~~(S//NF)~~ In a notice filed on July 13, 2015, the Government informed the Court that information acquired pursuant to the Foreign Intelligence Surveillance Act (FISA) that is subject to purge or age-off is being retained in two of NSA's compliance mission management systems, [redacted] and [redacted]. *See* "Update and Notice Regarding the National Security Agency's (NSA) purge process for FISA-acquired information in Mission Management Systems," (July 13, 2015) (hereinafter "July 2015 Notice"). One of the purposes of the July 2015 Notice was to update the Court on NSA's purge protocols, and certain changes thereto, with respect to certain mission management systems, including [redacted] and [redacted]. On October 8, 2015, the Honorable Thomas F. Hogan held a hearing to discuss a number of Section 702-compliance related issues, including the retention of data in [redacted] and [redacted] that is otherwise subject to purge. Following the hearing, on October 14, 2015, Judge Hogan issued an Order requiring the Government to explain in writing:

(a) How it justifies under NSA's 702 SMPs the retention and use in [redacted] and [redacted] of information otherwise subject to purge; and

(b) How it justifies under 50 U.S.C. § 1809(a)(2) the retention and use in [redacted] and [redacted] of information otherwise subject to purge.

See Order at 4. The Government herein provides additional background on [redacted] and [redacted], descriptions of the data contained therein and how it is used, changes the Government proposes to make to the destruction of data in those systems, and legal analysis in response to the Court's questions.

I. ~~(S//NF)~~ Background on [redacted] and [redacted]

~~(TS//SI//NF)~~ [redacted] and [redacted] are important compliance-related systems that help ensure the Government targets, under Section 702, only non-United States persons located outside the United States. [redacted][1]

~~(TS//SI//NF)~~ Specifically, [redacted] is a compliance tool that assists NSA personnel in [redacted] possibly indicative of a user being in the United States [redacted]. For example, [redacted]. [redacted] This information is then reviewed by NSA oversight and compliance personnel in order to make a determination regarding whether that event is actually indicative of a person [redacted] inside the United States.

~~(TS//SI//NF)~~ [redacted] is another tool that provides analysts with limited information regarding a target's current location [redacted]

[1] ~~(S//NF)~~ [redacted]

[redacted]

[2] ~~(TS//SI//NF)~~ [redacted]

[redacted]

A. ~~(S//NF)~~ Additional Background on NSA's Use of [redacted]

~~(TS//SI//NF)~~ [redacted] is critical for identifying indications that users of certain Section 702-tasked facilities may be located inside the United States, a process required by NSA's Section 702 Targeting Procedures.[3] To identify potential accesses from within the United States, [redacted]

[3] ~~(S//NF)~~ According to Section II of NSA's Targeting Procedures, NSA must "[r]outinely check[] all electronic communications [redacted] tasked pursuant to these procedures [redacted] to determine if an electronic communications [redacted] was accessed from inside the United States."

[4] ~~(S//NF)~~ [redacted]

[5] ~~(TS//SI//NF)~~ [redacted]

~~(TS//SI//NF)~~ [redacted] is used by NSA compliance and technical personnel actively involved in resolving possible indications of access from the United States, as well as analysts.[6] [redacted]

~~(TS//SI//NF)~~ [redacted]

[6] ~~(S//NF)~~ [redacted]

[7] ~~(TS//SI//NF)~~ [redacted]

[redacted]

~~(TS//SI//NF)~~ [redacted]

[redacted]

[8] ~~(TS//SI//NF)~~ [redacted].

[redacted]

~~(TS//SI//NF)~~ [redacted]

[redacted]

~~(TS//SI//NF)~~ [redacted]

[redacted]

[9] ~~(S)~~ According to Section I of NSA's Targeting Procedures: "Furthermore, in order to prevent the inadvertent targeting of a United States person, NSA [redacted]

[redacted]

~~(TS//SI//NF)~~ [redacted]

[redacted] As described in the Government cover filing to the 2014 Certifications,

[redacted] a significant volume [redacted] are resolved as not indicative of [redacted]. The volume of [redacted] varies, but NSA reports that, [redacted] on average more than [redacted] are typically generated each day (including from [redacted], approximately [redacted] of which on average are further prioritized [redacted] as potentially indicative of access originating from the

United States.[10] It is important to note that a single facility may generate [redacted] and not all [redacted] are indicative of compliance incidents. For example, since October 2013, NSA identified approximately [redacted] instances in which prior alert information resulted in alerts being prioritized as "urgent" and subject to priority review. [redacted]

~~(TS//SI//NF)~~ The Government acknowledges, however, that there are instances in which information retained [redacted] likely cannot be reasonably assessed to provide future assistance in resolving compliance-related issues. [redacted]

[10] ~~(S)~~ Although the number fluctuates, NSA reports that for 2014 more than 90% of the [redacted] generated were "false positives," *i.e.*, were determined after further NSA analysis not to be indicative of access of the facility by a user inside the United States.

B. ~~(S//NF)~~ Additional Background on NSA's Use of [redacted]

~~(S//NF)~~ [redacted] serves important compliance-related functions by helping prevent the tasking of facilities pursuant to Section 702 when those facilities are used by persons located in the United States, and assisting analysts to avoid querying United States person identifiers when not permitted by applicable minimization procedures. [redacted] Analysts with proper training and a mission need have access to the data in [redacted]

~~(TS//SI//NF)~~ [redacted]

~~(TS//SI//NF)~~ [redacted]

[11] ~~(S//NF)~~ [redacted]

[redacted]

~~(TS//SI//NF)~~ [redacted]

[redacted]

---

[12] ~~(TS//SI//NF)~~ [redacted].

[13] ~~(TS//SI//NF)~~ [redacted]

[redacted]

~~(TS//SI//NF)~~ [redacted]

II. ~~(S//NF)~~ Prospective Retention Plan

~~(TS//SI//NF)~~ The above Section describes NSA's current practice with respect to the retention of data in [redacted] and [redacted] In order to better align the retention of data in those systems with the Section 702 minimization procedures, and what the Government believes is permitted by Section 1809, below the Government proposes new retention practices for both [redacted] and [redacted] and provides an explanation as to why such retention is consistent with Section 1809 and the Section 702 minimization procedures.

A. ~~(S//NF)~~ [redacted]

~~(TS//SI//NF)~~ First, NSA will begin implementing in [redacted] the age-off time periods required by the Section 702 SMPs for all underlying records of FISA-acquired information. NSA will report to the Court when this is completed with respect

to historical data. Second, NSA will modify the manner in which it handles information subject to purge. Specifically, if the underlying data is subject to purge, NSA will limit access to such information in [redacted] to the following specific fields, which may contain FISA-acquired or derived information: [redacted] Importantly, although this specific information subject to purge will not be deleted from [redacted] access to this limited information will be restricted to compliance and technical personnel [redacted] and system administrators. In such cases, analysts will only see a notice indicating that the information has been purged. This will further ensure that the information subject to purge in [redacted] is not used for any other purpose, including [redacted].

B. ~~(S//NF)~~ [redacted]

~~(TS//SI//NF)~~ As with [redacted] NSA will begin implementing the age-off time periods required by the Section 702 SMPs in [redacted] for all underlying records drawn from other systems, as well as historical records of [redacted] queries. Additionally, NSA plans to modify its treatment of information collected pursuant to FISA-authorities and identified on the MPL. If the underlying data is subject to purge, NSA will delete from [redacted] both the underlying data and certain fields in the information presented to analysts in response to queries and limit access to such information in [redacted] to the following specific fields [redacted]

[redacted] From the underlying data, which will be purged going forward, [redacted] NSA also retains the dates that NSA analysts previously queried the facility in [redacted] and shows the above information to allow them to assess the timing of the access in the context of other known information. This further ensures that the information subject to purge in [redacted] is not used for any purpose other than collection avoidance. An example of what will be displayed to analysts is attached at Exhibit A.

III. (U) Relevant Provisions of FISA and Minimization Procedures

A. (U) Section 702 of FISA, 50 U.S.C. § 1881a

(U) Under Section 702, the Attorney General and Director of National Intelligence may authorize the targeting of non-United States persons reasonably believed to be located outside the United States. 50 U.S.C. § 1881a(a). Acquisitions conducted under Section 702 must comply with certain limitations enumerated in the statute. First and foremost among these limitations is that Section 702 acquisitions may not intentionally target any person known at the time of acquisition to be located in the United States. 50 U.S.C. § 1881a(b)(1). To ensure compliance with this limitation, the statute also requires the adoption and use of procedures ("targeting procedures") that are reasonably designed to ensure that Section 702 acquisitions are limited to targeting persons reasonably believed to be located outside the United States. 50 U.S.C. § 1881a(c)(1)(A), (d)(1).

(U) Another limitation imposed by Section 702 is that such acquisitions 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. 50 U.S.C. § 1881a(b)(4). Accordingly, Section 702 requires that the Government's targeting procedures be reasonably designed to comply with this requirement, too. 50 U.S.C. §

1881a(d)(1)(B). Although this limitation on its face applies regardless of whether the target is a party to a communication the Government seeks to acquire, to the extent that the target is a party to that communication, a reasonable belief that the target is located outside the United States, by itself, ensures compliance with this limitation. *See* [redacted] Opinion at 15 (noting that "because a user of a tasked selector is a party to every to/from communication acquired by NSA, a reasonable belief that the users of tasked selectors are outside the United States will ensure that NSA does not intentionally acquire any to/from communication 'as to which the sender and all intended recipients are known at the time of acquisition to be located in the United States.'" (citation omitted)).[14]

~~(S//NF)~~ While there are many aspects of NSA's Targeting Procedures designed to ensure compliance with these statutory limitations, particularly relevant to the [redacted] and [redacted] systems and the data discussed in this filing are the provisions in the Targeting Procedures governing pre-tasking checks and post-tasking checks. [redacted] Further, in conducting post-tasking analysis, the Targeting Procedures state that NSA will "routinely check[] all electronic communications [redacted] tasked pursuant to these procedures [redacted] to determine if an electronic communications [redacted] was accessed from inside the United

[14] ~~(S)~~ [redacted]

States." *Id.* at 8. In its opinion last year, this Court had occasion to reanalyze the post-tasking requirements and in particular NSA's processing [redacted], stating that "[d]iligent and prompt response to credible indications that a tasked facility has been accessed from the United States goes to the heart of the requirement of 50 U.S.C. § 1881a(d)(1)(A) that targeting procedures be reasonably designed to ensure that acquisitions target persons reasonably believed to be outside the United States." *See* [redacted] Opinion at 28-30.

(U) As the foregoing makes clear, foreignness determinations, both pre-tasking and post-tasking, are a fundamental element of Section 702's statutory scheme. Such determinations also contribute significantly to the Fourth Amendment reasonableness of Section 702 collection. *See, e.g.*, [redacted] Opinion at 37-38 (recognizing that "the targeting procedures reasonably confine acquisitions to targets who are non-U.S, persons outside the United States," and that "[s]uch persons are not protected by the Fourth Amendment" (*citing United States v. Verdugo-Urqidez*, 494 U.S. 259, 274-75 (1990)).

B. (U) 50 U.S.C. § 1809(a)(2)

~~(S//NF)~~ Section 1809 prohibits the Government from knowingly using information that was acquired in violation of FISA. *See* 50 U.S.C. § 1809(a)(2) (prohibiting the disclosure or use of "information obtained under color of law by electronic surveillance, knowing or having reason to know that the information was obtained through electronic surveillance [that was] not authorized" by statute).

[redacted]

[redacted]

[redacted]

[redacted]

C. (U) NSA's Section 702 SMPs

~~(S//NF)~~ Section 5 of NSA's Section 702 SMPs states: "Notwithstanding the above, if a domestic communication indicates that a target has entered the United States, NSA may promptly notify the FBI of that fact, as well as any information concerning the target's location that is contained in the communication. NSA may also use information derived from domestic communications for collection avoidance purposes, and may provide such information to the FBI and CIA for collection avoidance purposes. NSA may retain the communication from which such information is derived but shall restrict the further use or dissemination of the communication by placing it on the Master Purge List (MPL)." (emphasis added) As described above, this is precisely the process NSA has established [redacted]. The information subject to destruction is placed on the MPL but available [redacted] for collection avoidance purposes.

~~(S//NF)~~ As a result, NSA believed that its historic practices regarding retention of limited information [redacted] for collection avoidance purposes were compliant with its minimization procedures. In light of the concerns expressed by the Court in the Order, however, as addressed more fully below, the Government proposes to implement additional controls consistent with NSA's overall

[15] (U) Section 109 of FISA, as codified at 50 U.S.C. § 1809, prohibits the intentional disclosure or use of the results of unauthorized electronic surveillance but this section of the statute was enacted before Congress' enactment of Section 702 in 2008. Because Section 702(b) of FISA contains statutory limitations on how the Government may use Section 702 to effectuate surveillance directed against non-U.S. persons reasonably believed to be located outside the United States, to the extent there is any conflict between the requirements of Section 109 and Section 702(b), the Act as a whole should be interpreted in a complementary manner so as to reflect the clear desire of Congress that Section 702 not be used to target U.S. persons or persons located inside the United States.

compliance approach to Section 702 data regarding its limited retention and use of this information for collection avoidance purposes.

IV. ~~(S//NF)~~ The Nature of Collection Under Section 702 Requires Significant Use of Assessments [redacted] Consistent with Section 1809 and NSA's Section 702 SMPs.

(U) As described by the Privacy and Civil Liberties Oversight Board (PCLOB), "[t]he Section 702 program is a technically complex collection program with detailed rules embodied in the targeting procedures, minimization procedures, and Attorney General Guidelines regarding the targeting acquisition, querying, retention, and dissemination." PCLOB Section 702 Report at 77. The PCLOB also stated that it "has been impressed with the rigor of the Government's efforts to ensure that it acquires only those communications it is authorized to collect, and that it targets only those persons it is authorized to target. Moreover, the Government has taken seriously its obligations to establish and adhere to a detailed set of rules regarding how it handles United States person communications that it acquires under the program." PCLOB Section 702 Report at 103. The information [redacted] are part of the Government's recognized effort to comply with the targeting procedures and thereby avoid unauthorized surveillance.

(U) As noted above, the Section 702 statutory framework, and thus the relevant Section 702 targeting procedures, are designed to protect United States persons and United States-person information from improper targeting and use. As PCLOB recognized, the "[FISC]-approved targeting rules and multiple layers of oversight" were factors underpinning its conclusion that the Section 702 program "fits within the 'totality of the circumstances' standard for reasonableness under the Fourth Amendment." PCLOB Section 702 Report at 9.

~~(S//NF)~~ By retaining the limited Section 702-acquired information [redacted], even if the underlying data is subject to destruction, the NSA may be able to resolve [redacted] in a more timely manner and/or avoid targeting individuals located in the United States. For example, [redacted]

A. (U) Retention of data in [redacted]

~~(S//NF)~~ The Government believes the exception recognized [redacted] should apply to Section 1809 data retained in [redacted] The Section 702 statutory framework, and thus the relevant Section 702 targeting procedures, are designed to protect United States persons and United States-person information from improper targeting and use. Furthermore, the use of Section 702-acquired information, even that which is unlawfully acquired, is already permitted by NSA's Targeting Procedures in limited instances.

~~(TS//SI//NF)~~ [redacted]

[16] ~~(S)~~ According to Section I of NSA's Targeting Procedures: "Furthermore, in order to prevent the inadvertent targeting of a United States person, NSA [redacted]

[redacted] Similarly, the Government believes that retaining the limited Section 702-acquired information subject to destruction [redacted] is appropriate for the following three reasons.

1. ~~(S//NF)~~ **The Limited Access to, and the Purpose of, [redacted] Safeguards Against Further Use or Dissemination of the Information.**

~~(TS//SI//NF)~~ First, access to information [redacted] is limited to NSA personnel actively involved in resolving possible indications of access from the United States. As further described below, going forward any information subject to purge [redacted] will be made accessible only to compliance and technical personnel actively working [redacted].[17] Thus, the information will only ever be used to resolve a potential compliance incident and, thus, will not be used in preparation of FISA applications, the drafting of reports, or the targeting of Section 702 selectors.

2. ~~(S//NF)~~ **The Scope of Section 702 Requires Significant Analysis of Data for Compliance Purposes.**

~~(TS//SI//NF)~~ Section 702 has a much different statutory framework than Title I/III of FISA. Because the Government must maintain, under a totality of the circumstances, a reasonable basis to conclude that all users of a facility are non-United States persons located outside the United States, the Government must be able to retain data that may bear directly on that conclusion. [redacted] is a required and invaluable part of NSA's implementation of the post-targeting obligations contained in its targeting procedures. Although Section 1809 is intended to prohibit the future use of the results of unauthorized surveillance, given the importance of this data to ensuring future compliance with the requirements of Section 702, requiring NSA to parse through

[17] ~~(S)~~ [redacted]

[redacted] in an attempt to determine whether there is a known, reasonable basis to believe the information associated with each alert will be relevant to a future incident, would in this limited context go beyond the purpose served by Section 1809. While NSA will be able to make that assessment in some cases, and not in others, the vast majority [redacted] are impossible to assess. Thus, in the context of Section 702 compliance, NSA cannot reasonably be expected to know in advance the future travel plans of Section 702 targets. NSA's analysis of new [redacted] directly benefit from information [redacted] regarding prior [redacted] including past assessments by compliance and technical personnel as to whether any [redacted] is indicative of a target's location. As such, the Government believes the above-described data is appropriately retained [redacted].

~~(TS//SI//NF)~~ The Government acknowledges that the retention of all Section 702-acquired alert information [redacted], even though some of that information is derived from data that implicates Section 1809, means that NSA will not be engaging in a case-by-case, or [redacted] analysis. [redacted]. The Government also acknowledges that without such case-by-case analysis, there will likely be instances in which there is no basis to assess that [redacted] will be helpful in resolving future incidents or otherwise prohibit/reduce future incidents of non-compliance [redacted]. However, given the overall purpose of Section 702, the role [redacted] plays in preventing unauthorized surveillance as part of the operation of this collection, the complex range of circumstances in which this data may be used to

avoid such future unauthorized collection, and the difficulty of parsing through it in advance to make those determinations, the Government submits the retention of Section 702-acquired information [redacted] is consistent with the narrow exception laid out [redacted].

3. ~~(S//NF)~~ The SMPs Allow Retention of Data Otherwise Subject to Purge [redacted].

~~(TS//SI//NF)~~ When targeting individuals pursuant to Section 702, NSA may acquire data that is required to be purged pursuant to NSA's minimization procedures, but is not unauthorized electronic surveillance. [redacted]

[redacted]

~~(S//NF)~~ Because such data does not implicate Section 1809,[18] domestic communications, as defined by NSA's Section 702 minimization procedures, may be retained in the manner permitted by the procedures. As indicated above, Section 5 permits NSA to "use information derived from domestic communications for collection avoidance purposes" as long as other uses or disseminations are prohibited. As detailed above, this is the process NSA has established [redacted]. The information subject to destruction is placed on the MPL but available [redacted] for collection avoidance purposes.

---

[18] ~~(S//NF)~~ Because such data does not implicate the prohibitions in Section 1809, the Government is able to use the information pursuant to its minimization procedures. *See, e.g.*, NSA Section 702 SMPs § 5 (waiver provision).

~~(TS//SI//NF)~~ While some [redacted] subject to purge [redacted] are domestic communications, others may not be. [redacted]

[redacted]

B. ~~(S//NF)~~ Retention of Data [redacted].

~~(S//NF)~~ As with [redacted] the Government believes the exception recognized [redacted] should apply to Section 1809 data retained in [redacted] Unlike [redacted] however, [redacted] is available to the analytic workforce, which uses it on a daily basis to help properly implement of Section 702 by ensuring collection is directed only at non-United States persons located overseas. Given the manner in which [redacted] is used to ensure compliance with Section 702 targeting restrictions, and the extremely limited nature of the information proposed to

be retained, the Government believes the retention of Section 702-acquired data in [redacted] is consistent [redacted].

1. (U) **There is Compliance Value in the Results from Historic [redacted] Queries.**

~~(TS//SI//NF)~~ First, the limited amount of Section 702-acquired data [redacted] that is derived from data subject to Section 1809 retains compliance-related value.[19] [redacted]

~~(S//NF)~~ Second, there is no significant utility, when compared to the articulated purpose of Section 1809, for requiring NSA to parse through [redacted] and attempt to determine whether there is a known, reasonable basis to believe the information will be relevant to any future compliance matters. While NSA will be able to make that assessment in some cases, and not in others, the vast majority of results, as with [redacted] will be impossible to assess in advance. NSA cannot be reasonably expected to know all future foreign intelligence priorities (which will impact where NSA devotes resources), the future content review by analysts (which will

[19] ~~(S//NF)~~ [redacted]

dictate what facilities are be subject to future [redacted] queries), or subsequent due diligence efforts undertaken by an analyst (which would impact the relevance of a prior result [redacted]. Because significant resources would be required before any such analysis could be contemplated on a [redacted], the fact that such analysis will be subject to unknown future elements, and the possible value of the very limited information [redacted] to a future compliance-related activity, the Government believes the above-described data is appropriately retained [redacted]

As noted above with respect to [redacted] this would not involve a case-by-case, or [redacted], analysis and thus could result in instances in which there is no reasonable basis to assess that a particular [redacted] query will be helpful in resolving future incidents or otherwise prohibit/reduce future incidents of non-compliance [redacted]. However, as with [redacted] the Government submits that given the overall purpose of Section 702, and the role [redacted] plays in preventing unauthorized surveillance as part of the operation of this collection, that the retention of the *de minimis* Section 702-acquired information [redacted] (which in some instances may be derived from data subject to Section 1809) is consistent with the narrow exception laid out [redacted].

2. ~~(S//NF)~~ The Section 702 Minimization Procedures Authorize the Retention of Data [redacted].

~~(TS//SI//NF)~~ As in the [redacted] described above, NSA may acquire data that is required to be purged pursuant to NSA's minimization procedures, but is not unauthorized collection. Because such data does not implicate Section 1809, any domestic communication (only some of the information subject to purge [redacted] will be a domestic communication) may be retained as permitted by NSA's Section 702

SMPs. As indicated above, Section 5 permits NSA to "use information derived from domestic communications for collection avoidance purposes" as long as other uses or disseminations are prohibited. While derived information is [redacted], the underlying information subject to destruction is placed on the MPL, and NSA may not use such results [redacted] for purposes other than compliance-related, including to support Title I/III tasking, reporting, or Section 702 tasking.

~~(TS//SI//NF)~~ While some results subject to purge [redacted] are domestic communications, others may not be. [redacted]

V. (U) CONCLUSION

(U//FOUO) For all the above reasons, the Government respectfully submits that the retention practices by NSA for data in [redacted] and [redacted] discussed above, are consistent with Section 1809 and the Section 702 minimization procedures. As made clear in the foregoing discussion, NSA's purpose for retaining information in these two compliance systems that may otherwise be subject to purge is for the narrow, limited purpose of preventing the very types of targeting errors that were of most concern to Congress when it enacted Section 702(b) of FISA.

Respectfully submitted,

Stuart J. Evans
Deputy Assistant Attorney General

By: _____
Kevin J. O'Connor
Chief, Oversight Section
Office of Intelligence
National Security Division
U.S. Department of Justice

All withheld information exempt under (b)(1) and (b)(3) unless otherwise noted. Approved for Public Release

VERIFICATION

(TS//SI//NF) I declare under penalty of perjury that the foregoing is true and correct. Executed pursuant to Title 28 United States Code, § 1746 on 21 Oct 2015.

[redacted]

Deputy Director, Signals Intelligence Directorate
National Security Agency

ACLU 16-CV-8936 (RMB) 000896

ATTACHMENT A

[redacted]