

reveal classified information. As a result, I have determined that no portion of the documents could be reasonably segregated and released.

41. The withheld information is also protected from release by statute and is exempt from release based on FOIA Exemption 3, 5 U.S.C. § 552(b)(3). Specifically, there are three Exemption 3 statutes that protect from public release the technical means by which NSA effects its collection operations: 50 U.S.C. § 3605, 18 U.S.C. § 798, and 50 U.S.C. § 3024(i)(1).

42. The withheld information clearly relates to a “function of the National Security Agency.” 50 U.S.C. § 3605. Indeed, this information relates to one of NSA’s primary functions, its SIGINT mission. Any disclosure of the withheld information regarding this intelligence source, and information regarding related methods would reveal NSA’s capabilities and the tradecraft used to carry out this vital mission. Further, revealing these details would disclose “information with respect to [NSA’s] activities” in furtherance of its SIGINT mission. 50 U.S.C. § 3605.

43. Moreover, this information is protected from public release pursuant to 50 U.S.C. § 3024(i)(1), which states that “[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.” The withheld information concerns the intelligence sources and methods used by NSA to carry out its core foreign intelligence mission — *i.e.*, the means by which NSA acquires communications and derives useful foreign intelligence therefrom. Therefore, this information falls squarely within the protection of § 3024(i)(1) and should be afforded absolute protection from release.

44. Finally, the information is protected from release under 18 U.S.C. § 798, which protects from disclosure classified information concerning the communications intelligence activities of the United States, or information obtained by communications intelligence

processes. Disclosure of the withheld information about this intelligence source, and the related methods, would reveal key information about the means through which NSA collects and processes communication intelligence, thereby falling within the scope of protection offered by this statute.

Legal Opinions

45. NSA withheld from disclosure information relating to legal analyses of NSA collection and analysis programs and activities written by the NSA OGC or NSD. The documents in this category include NSA Documents 7, 9, 14, 15, 16, 17, 18, 19, 20, 21, and 28, and NSD Document 31. Each of these documents contains details regarding SIGINT sources and methods and legal analysis relating to those sources and methods. For most of the documents, the titles themselves are classified because the titles alone would reveal information about intelligence sources, such as the technical means by which communications are collected, and methods, such as analytic techniques applied to collected data. Unclassified descriptions of each document, including the date, number of pages, and serial numbers (where applicable) were released. NSA withheld details regarding the manner in which NSA selects its foreign intelligence targets, the technical means by which NSA collects communications intelligence, as well as the analytical tools and processes employed by NSA analysts to extract useful foreign intelligence from raw data.

46. With respect to NSA Documents 7, 9, 14, 15, 18, and 21, as well as NSD Document 31, I have determined that each document is currently and properly classified in its entirety at the TOP SECRET level in accordance with EO 13526, because the release of this information could reasonably be expected to cause exceptionally grave damage to the national security. Information contained in these documents pertains to intelligence activities, intelligence

sources or methods, or cryptology, or the vulnerabilities or capabilities of systems or projects relating to the national security and therefore meets the criteria for classification set forth in Sections 1.4(c) and 1.4(g) of EO 13526.

47. With respect to NSA Documents 16, 17, 19, and 20, and the withheld portions of NSA Document 28 (**AEX 14**) marked with a (b)(1) exemption code, I have determined that each is currently and properly classified at the SECRET level in accordance with EO 13526, because the release of this information could reasonably be expected to cause serious damage to the national security. Information contained in these documents pertains to intelligence activities, intelligence sources or methods, or cryptology, or the vulnerabilities or capabilities of systems or projects relating to the national security and therefore meets the criteria for classification set forth in Sections 1.4(c) and 1.4(g) of EO 13526. *See supra*, ¶ 30.

48. Disclosure of the operational information withheld here would reveal a wide variety of details that could be used to counter NSA foreign intelligence activities, and cause serious harm to national security. As discussed above, disclosure of the technical details by which NSA effects SIGINT collection, the scope of that collection, and the analytic techniques applied to the collected data would demonstrate the capabilities and limitations of the U.S. SIGINT system, the success (or lack of success) in acquiring certain types of communications, and the ability (or lack thereof) of NSA to derive useful foreign intelligence information from particular categories of data. Once alerted to these methods, adversaries could develop additional countermeasures to thwart collection of electronic communications or hinder NSA's ability to derive useful foreign intelligence therefrom. Such a reaction may result in denial of access to targets' communications and loss of information critical to the national security and defense of the United States.

49. The information withheld in the documents listed in paragraph 45 is also protected from release by statute and exempt from release based on FOIA Exemption 3, 5 U.S.C. § 552(b)(3), and specifically, the three Exemption 3 statutes discussed above: 50 U.S.C. § 3605, 50 U.S.C. § 3024(i)(1), and 18 U.S.C. § 798.

50. Information regarding NSA's collection of communications and analytic capabilities relate to a "function of the National Security Agency," 50 U.S.C. § 3605. Indeed, such information relates to one of NSA's primary functions, its SIGINT mission. The withheld operational information, if revealed, would also disclose "information with respect to [NSA's] activities" in furtherance of its SIGINT mission. 50 U.S.C. § 3605.

51. Moreover, this information is protected from public release pursuant to 50 U.S.C. § 3024(i)(1), which states that "[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure." The withheld operational details, such as the technical means of collection and analytic methodology, constitute the sources and methods used by NSA to carry out its SIGINT mission. Therefore, this information falls squarely within the protection of § 3024(i)(1) and should be afforded absolute protection from release.

52. Additionally, this information is protected from release under 18 U.S.C. § 798, which protects from disclosure classified information concerning the communications intelligence activities of the United States, or information obtained by communications intelligence processes. Disclosure of the means by which NSA collects communications, and the analytic techniques applied to collected data, would reveal the sources and methods at the core of the U.S. Government's communications intelligence activities, thereby falling within the scope of protection offered by this statute.

53. Finally, NSA Documents 7, 14, 15, 16, 17, 18, 19, 20, 21, and 28 contain correspondence between NSA OGC and its internal clients, such as the Signals Intelligence Directorate, the NSA organization tasked with carrying out NSA's SIGINT mission, which is protected under Exemption 5 of the FOIA because this correspondence includes privileged communications between Agency attorneys and Agency clients.⁶ "The attorney-client privilege protects communications (1) between a client and his or her attorney (2) that are intended to be, and in fact were kept confidential (3) for the purpose of obtaining or providing legal assistance." *Brennan Center for Justice at New York Univ. Sch. of Law v. U.S. Department of Justice*, 697 F.3d 184, 203 (2d Cir. 2012). The communications at issue were made in order to provide legal advice to Agency clients on a variety of operational issues that arose under EO 12333, the communications were made in confidence, and have not since been used to publically justify NSA actions or expressly adopted as Agency policy.

54. The legal analyses in all of the documents listed in Paragraph 45, with the exception of NSA Document 28, are inextricably intertwined with the factual descriptions of NSA functions and activities and classified operational details that gave rise to the questions being considered, so there are no reasonably segregable, non-exempt portions of those documents.

55. Unlike the other documents listed in Paragraph 45, NSA determined that Document 28 was reasonably segregable, and therefore released it in part. I have reviewed this decision and determined that it remains correct. The withholdings in Document 28 were narrowly tailored to protect operational details regarding the SIGINT activities of NSA and privileged legal analysis and advice provided by NSA attorneys to NSA clients, as described

⁶ NSA is not claiming that any portion of NSA Document 9 or NSD Document 31 is exempt from release under Exemption 5.

above. The limited information withheld in this document is exempt from release under Exemptions 1, 3, and 5 (as indicated by the exemption codes listed in the document) for the reasons described above.⁷ All information withheld pursuant to Exemption 5 is independently exempt from public release based on Exemptions 1 and/or 3 of the FOIA.

NSD Document 4

56. NSD fully withheld Document 4 on its *Vaughn* index in part because the release of any portion of that document would disclose classified information about functions or activities of NSA. The document is a 20-page document dated 20 November 2007 and is described as “NSD Legal Memo on Amending DoD Procedures and Accompanying Documentation.” This document, including its full title, was withheld in full under Exemption 1 and Exemption 3. I have reviewed the information withheld and determined that the information is currently and properly classified at the SECRET level in accordance with EO 13526 because the release of this information could reasonably be expected to cause serious damage to the national security. The information withheld pertains to intelligence activities, intelligence sources or methods, or cryptology, or the vulnerabilities or capabilities of systems or projects relating to the national security and therefore meets the criteria for classification set for in Sections 1.4(c) and 1.4(g) of EO 13526. The harm to national security of releasing any portion of this document and the reasons that no portion of this document can be released without disclosing classified information cannot be fully described on the public record. As a result, my *ex parte, in camera* classified declaration more fully explains why this document was withheld in full.

⁷ Certain paragraphs withheld in NSA Document 28 were mistakenly marked with only Exemption 5 codes (*see* pgs. 3 and 7). Nevertheless, those paragraphs are also exempt from disclosure under Exemption 3, specifically 50 U.S.C. § 3605, because they describe NSA functions or activities. A properly marked copy of NSA Document 28 is included in the set of documents attached hereto.

57. The information withheld in NSD Document 4 also relates to a “function of the National Security Agency,” 50 U.S.C. § 3605. Indeed, this information relates to one of NSA’s primary functions, its SIGINT mission. Any disclosure of the withheld information would reveal NSA’s capabilities and the tradecraft used to carry out this vital mission. Further, revealing these details would disclose “information with respect to [NSA’s] activities” in furtherance of its SIGINT mission. 50 U.S.C. § 3605. Therefore, the information withheld is also protected from release by statute and is exempt from release based on FOIA Exemption 3, 5 U.S.C. § 552(b)(3).

OIG Report ST-09-0019

58. NSA fully withheld NSA OIG Report ST-09-0019, NSA Document 23, because it is fully exempt from disclosure pursuant to FOIA Exemptions 1 and 3. The document is an 84-page report by the NSA OIG concerning particular intelligence activities of the NSA, including the dissemination of communications intelligence to partner agencies. The report contains granular detail regarding the nature of NSA’s intelligence partnerships, the types and amount of communications intelligence it collects and disseminates, the names of particular NSA targets, the structure of NSA’s SIGINT databases, and suggestions by the OIG on how to improve the dissemination of SIGINT to partner agencies. NSA determined that there is no reasonably segregable, non-exempt information in the report.

59. I have reviewed NSA’s withholding in full of this document and determined both that this decision was correct and that the entirety of this document remains currently and properly classified at the TOP SECRET level in accordance with EO 13526 as its release of this could reasonably be expected to cause exceptionally grave damage to the national security. The information withheld pertains to intelligence activities, intelligence sources or methods, or cryptology, foreign activities of the United States, or the vulnerabilities or capabilities of systems

or projects relating to the national security and therefore meets the criteria for classification set forth in Sections 1.4(c), 1.4(d) and 1.4(g) of EO 13526.

60. Disclosure of the types and amount of communications intelligence NSA collects and disseminates, and the names of particular NSA targets whose information has been disseminated, would demonstrate the capabilities and limitations of the U.S. SIGINT system, and the success (or lack of success) in acquiring certain types of communications. The collection of communications intelligence is central to NSA's mission and allows NSA to provide unique and timely insight into the activities of foreign adversaries for U.S. policymakers. Public disclosure of NSA's capabilities to acquire specific types of communications would alert targets to the vulnerabilities of their communications (and conversely, which of their communications are not vulnerable). Foreign intelligence targets know how they communicate, so disclosure of this information would permit foreign adversaries to more effectively craft their communications security efforts to frustrate the Government's collection of information crucial to the national security.

61. Additionally, all of the information described above relates to a "function of the National Security Agency," 50 U.S.C. § 3605, and is therefore also protected from release by FOIA Exemption 3. Indeed, this information relates to one of NSA's primary functions, its SIGINT mission. A crucial part of NSA's SIGINT mission involves the dissemination of communications intelligence to partner agencies. In addition, NSA further protected this information based on 50 U.S.C. § 3024(i)(1), which states that the Director of National Intelligence "shall protect intelligence sources and methods from unauthorized disclosure." Finally, this information is protected from release under 18 U.S.C. § 798, which protects from disclosure information concerning the communications intelligence activities of the United

States, or information obtained by communications intelligence processes. Any disclosure of the withheld information would reveal NSA's capabilities and the tradecraft used to carry out its vital communications intelligence mission.

Intelligence Oversight Board Report-Fiscal Year 2013, 1st Quarter

62. NSA released, in part, 47 quarterly reports and 4 annual reports to the IOB from the 4th quarter of Fiscal Year ("FY") 2001 to the 2nd quarter of FY2013.⁸ The release of these reports totaled 617 pages. NSA conducted a line-by-line review of each report and released all reasonably segregable, non-exempt information. Of these 51 reports, Plaintiffs selected the quarterly report covering the 1st quarter of FY2013 for inclusion in the litigation sample.⁹ **AEX 15.**

63. The IOB reports discuss NSA intelligence activities undertaken pursuant to a variety of legal authorities, including EO 12333 and various portions of the Foreign Intelligence Surveillance Act (FISA), as amended. Plaintiffs' FOIA request only sought information pertaining to electronic surveillance undertaken pursuant to EO 12333. Therefore, none of the information concerning NSA activities undertaken pursuant to FISA authority is responsive to Plaintiffs' request. Nevertheless, NSA processed all portions of the document for release, consistent with Department of Defense policy.

64. The limited information withheld from disclosure concerns technical details regarding the methods by which NSA collects communications intelligence, information regarding the structure of NSA's SIGINT databases, including the means by which U.S.

⁸ Executive Order 12333, as amended, requires IC elements to report to the IOB intelligence activities they have reason to believe may be unlawful or contrary to Executive Order or Presidential Directive. In general, each NSA report contains similar categories of information, including an overview of recent oversight activities conducted by NSA's OIG and OGC; signals intelligence activities affecting certain protected categories; and descriptions of specific incidents which may have been unlawful or contrary to applicable policies.

⁹ This IOB report is NSA Document 79 and Bates Number 4165220.

Intelligence Community personnel query NSA SIGINT databases, information that would tend to reveal when a particular collection or analytic activity took place, information regarding the scope of NSA's collection activities, and information regarding the internal organization of NSA, including names of the offices involved in these programs. *See supra*, ¶ 33.

65. I have reviewed NSA's withholding of this limited information, which is owned by, produced by, or under the control of the U.S. Government, and determined both that this decision was correct and that the withheld information remains currently and properly classified at levels ranging from CONFIDENTIAL to TOP SECRET in accordance with EO 13526, because the release of this information could reasonably be expected to cause either damage, serious damage, or exceptionally grave damage to the national security. Each paragraph is marked with the level of classification appropriate for that section. Revealing technical details regarding the methods by which NSA collects communications intelligence, information regarding the structure of NSA's SIGINT databases, including the means by which U.S. IC personnel query NSA SIGINT collection systems,¹⁰ information that would tend to reveal when a particular collection or analytic activity took place, and information regarding the scope of NSA's collection activities could permit adversaries to develop countermeasures to frustrate NSA's collection of their communications or hinder NSA's ability to develop useful foreign intelligence from collected data. Moreover, information regarding the scope of NSA's collection activities, and the dates associated with collection, analysis, and deletion of collected communications, would reveal the ability of NSA to collect certain foreign intelligence information and the gaps in NSA's abilities.

¹⁰ "Querying" refers to the process of searching NSA's signals intelligence systems. The process of constructing and executing queries is tightly regulated and subject to rigorous technical and human audit controls.

66. Adversaries are known to study publicly released information about NSA activities. If those adversaries were made aware of the tradecraft employed by NSA, they could copy or mimic such tradecraft and direct it against the United States and its interests. Additionally, foreign intelligence targets know how they communicate, so disclosure of this information would permit foreign adversaries to more effectively craft their communications security efforts to frustrate the Government's collection of information crucial to the national security. Such a reaction may result in a loss of information critical to the national security and defense of the United States. Therefore, this information meets the criteria for classification set forth in Sections 1.4(c) and 1.4(g) of EO 13526.

67. All of the withheld information, including information regarding dates of specific NSA activities, and the names of NSA personnel or organizations, is also protected from release by statute and is exempt from release based on FOIA Exemption 3, 5 U.S.C. § 552(b)(3), and specifically, the three Exemption 3 statutes discussed previously: 50 U.S.C. § 3605, 18 U.S.C. § 798, and 50 U.S.C. § 3024(i)(1).

68. The information described above relates to a "function of the National Security Agency." 50 U.S.C. § 3605. Indeed, this information relates to one of NSA's primary functions, its SIGINT mission. Any disclosure of the withheld intelligence sources and related methods would reveal NSA's capabilities and the tradecraft used to carry out this vital mission. Further, revealing these details would disclose "information with respect to [NSA's] activities" in furtherance of its SIGINT mission. 50 U.S.C. § 3605. All of the information withheld under Exemption 3 (as indicated by the exemption codes) is protected from release by this statute.

69. Moreover, portions of the withheld information, as indicated by the specific exemption codes included in the released version of the report, is protected from public release

pursuant to 50 U.S.C. § 3024(i)(1), which states that “[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure.” The withheld information constitutes the sources and methods used by NSA to carry out its SIGINT mission. Therefore, this information falls squarely within the protection of 50 U.S.C. § 3024(i)(1) and should be afforded absolute protection from release.

70. Finally, as indicated by the exemption codes applied to portions of the IOB report, parts of the document are protected from release under 18 U.S.C. § 798, which protects from disclosure classified information concerning the communications intelligence activities of the United States, or information obtained by communications intelligence processes. Disclosure of the withheld information about NSA’s intelligence sources and methods would reveal key information about the means through which NSA collects and processes communication intelligence, thereby falling within the scope of protection offered by this statute.

Classified Annex to DoD Procedures, United States Signals Intelligence Directive 18,
and SMD 432

71. NSD produced the 1988 Classified Annex to the DoD Procedures under EO 12333, which had been previously processed and released in part by NSA and ODNI in September 2014.¹¹ Further, NSA released, in part, the 2011 version of USSID SP0018,¹² Appendix J to USSID SP0018,¹³ and Signals Intelligence Directorate Management Directive (SMD) 432.¹⁴ Each of these documents implements EO 12333 and prescribes policies and procedures for ensuring that SIGINT is conducted in accordance with the EO and applicable law. The Classified Annex to the DoD Procedures under EO 12333 supplements the rules for SIGINT collection, retention, and dissemination established by DoD Directive 5240.01 and DoD 5240.1-

¹¹ The Classified Annex is NSD Bates Number NSD094-125.

¹² USSID SP0018 is Bates Number 4086222 and attached to this declaration at **AEX 16**.

¹³ Appendix J is Bates Number 4086223 and attached to this declaration at **AEX 17**.

¹⁴ SMD 432 is NSA Document 5 and attached to this declaration at **AEX 18**.

R, which govern intelligence activities conducted by DoD components, such as NSA, that affect United States persons. USSID SP0018 prescribes policies and procedures and assigns responsibilities to ensure that the missions and functions of the United States SIGINT System (USSS) are conducted in a manner that safeguards the rights of U.S. persons, consistent with the Constitution, federal statutes, and EO 12333. Appendix J to USSID SP0018 establishes the procedures for USSS monitoring of radio communications of suspected international narcotics traffickers. SMD 432 is a policy of NSA's SIGINT Directorate that establishes procedural guidelines for collection and dissemination of SIGINT connected to U.S. field exercises. NSA redacted only limited information in these four documents and released all reasonably segregable, non-exempt information. The information withheld from these documents pertains to details of how NSA targets certain communications for collection, the types of facilities that NSA may target, and the types of communications that NSA can collect in specific circumstances.

72. I have reviewed the withholding of information in these documents and determined both that this decision was correct and that the information withheld remains currently and properly classified at the CONFIDENTIAL or SECRET levels in accordance with EO 13526, as indicated by the various portion markings in the documents, because the release of this information could reasonably be expected to cause damage, or serious damage, to the national security. Information contained in these documents pertains to intelligence activities, intelligence sources or methods, or cryptology, or the vulnerabilities or capabilities of systems or projects relating to the national security and therefore meets the criteria for classification set forth in Sections 1.4(c) and 1.4(g) of EO 13526.

73. Disclosure of the methods by which NSA determines which persons and facilities are of foreign intelligence value and the procedures by which particular communications are targeted would reveal information from which targets could derive countermeasures to evade NSA surveillance by masquerading as persons whose communications either explicitly are not or may not be authorized for collection. Appropriately targeting communications remains a primary requirement under all of NSA's authorities. As a result, revealing the precise methods and procedures by which NSA determines that it is authorized to target particular communications could encourage adversaries to adopt countermeasures that would make it more difficult for NSA to determine accurately the nature of their communications, such as the foreignness of those communications, thereby hindering the Government's collection of information crucial to the national security of the United States. Additionally, disclosure of the specific sources from which communications may be collected would alert the targets to which communications NSA did and did not collect, as well as reveal the nature and scope of NSA communications intelligence activities. Disclosure of this information would allow targets to discern which of their communications may have been collected, as well as gaps in collection that could reveal that particular communications were "safe."

74. Finally, disclosure of the technical details regarding the types of communications that NSA may collect would demonstrate the capabilities and limitations of the U.S. SIGINT system, and the success (or lack of success) in acquiring certain types of communications. The collection of communications intelligence is central to NSA's mission and allows NSA to provide unique and timely insight into the activities of foreign adversaries for U.S. policymakers. Public disclosure of NSA's capabilities to acquire specific types of communications, and the technical means and methods by which such acquisitions are effected,

would alert targets to the vulnerabilities of their communications (and conversely, which of their communications are not vulnerable). Once alerted, adversaries could develop additional countermeasures to thwart collection of electronic communications. Such a reaction may result in denial of access to targets' communications and therefore result in a loss of information critical to the national security and defense of the United States.

75. Much of this information, as indicated by unique exemption codes applied to each withholding, is also protected from release by statute and therefore is exempt from release based on the FOIA Exemption 3, 5 U.S.C. § 552(b)(3), statutes: 50 U.S.C. § 3605, 18 U.S.C. § 798, and 50 U.S.C. § 3024(i)(1).

76. The information described above relates to a "function of the National Security Agency." 50 U.S.C. § 3605. Indeed, this information relates to one of NSA's primary functions, its SIGINT mission. Any disclosure of the withheld operational details would reveal NSA's capabilities and the tradecraft used to carry out this vital mission. Further, revealing these details would disclose "information with respect to [NSA's] activities" in furtherance of its SIGINT mission. 50 U.S.C. § 3605.

77. Moreover, portions of the withheld information, as indicated by the specific exemption codes included in the released version of the documents, is protected from public release pursuant to 50 U.S.C. § 3024(i)(1), which states that "[t]he Director of National Intelligence shall protect intelligence sources and methods from unauthorized disclosure." The withheld information constitutes the sources and methods used by NSA to carry out its SIGINT mission. Therefore, this information falls squarely within the protection of 50 U.S.C. § 3024(i)(1) and should be afforded absolute protection from release.

78. Finally, as indicated by the exemption codes claims for portions of the documents, some of the withheld information is protected from release under 18 U.S.C. § 798, which protects from disclosure classified information concerning the communications intelligence activities of the United States, or information obtained by communications intelligence processes. Disclosure of the withheld information about NSA's intelligence sources and methods would reveal key information about the means through which NSA collects and processes communication intelligence, thereby falling within the scope of protection offered by this statute.

Records Referred by the Federal Bureau of Investigation (FBI)

79. FBI referred a number of documents to NSA for review in connection with this litigation. Of those, it is my understanding that Plaintiffs have challenged only the document identified at FBI Bates Numbers 30-35 and described by FBI as "Electronic Communication from the FBI's Office of General Counsel, National Security Law Branch to all FBI Offices setting out the policy and procedure for requesting Attorney General authority under Executive Order 12333, Section 2.5 to collect intelligence on U.S. persons overseas." NSA requested that FBI withhold a portion of page 3 of that document on behalf of NSA. I have determined that the information that NSA requested be withheld is exempt from disclosure pursuant to FOIA Exemptions 1 and 3. The portion of that document withheld at NSA's request concerns information about an intelligence target that is operationally useful to NSA in effecting communications surveillance. That information is currently and properly classified at the SECRET level in accordance with EO 13526, because the release of this information could reasonably be expected to cause serious damage to the national security, as described in greater detail above in Paragraphs 73 and 74. The operational details of NSA communications

intelligence activities constitute information about intelligence activities, intelligence sources or methods, or cryptology, or the vulnerabilities or capabilities of systems or projects relating to the national security and therefore meet the criteria for classification set for in Sections 1.4(c) and 1.4(g) of EO 13526. *See supra* ¶ 30. Moreover, these classified operational details of NSA communications intelligence activities, including intelligence sources and methods, are also protected from release by statute and therefore are exempt from release based on the FOIA Exemption 3 statutes: 50 U.S.C. § 3605, 18 U.S.C. § 798, and 50 U.S.C. § 3024(i)(1). *See supra*, ¶¶ 32-36.

Records Referred by the DOJ Office of Legal Counsel (OLC)

80. OLC, in response to its separate stipulation with Plaintiffs, identified several documents that contain NSA information and referred those documents to NSA for review. Of those, it is my understanding that Plaintiffs have challenged certain OLC documents containing NSA information, identified on the OLC Index as OLC 2, 3, 4, 6, 8, 9, and 10, and NSD Document 36, which is also an OLC memorandum. I have reviewed this matter and determined that each of these documents contains some information that is exempt from release pursuant to Exemptions 1 and 3, because the information is currently and properly classified under EO 13526 and because its disclosure would reveal intelligence sources and methods protected by the National Security Act and the NSA Act of 1959. This information is currently and properly classified at the levels ranging from SECRET to TOP SECRET in accordance with EO 13526 because the release of this information could reasonably be expected to cause either serious or exceptionally grave damage to the national security. Information withheld from these documents concerns the identities of NSA surveillance targets and the scope of NSA collection, including specific types of communications the NSA can and cannot collect under particular

surveillance programs. This information pertains to intelligence activities, intelligence sources or methods, or cryptology, or the vulnerabilities or capabilities of systems or projects relating to the national security and therefore meets the criteria for classification set forth in Sections 1.4(c) and 1.4(g) of EO 13526. Disclosure of the identities of NSA targets and the scope of NSA collection would reveal the capability of NSA and the IC to collect information about these targets and alert our adversaries about whether certain past communications are, or are not, likely to have been targeted and captured. Additionally, this classified information, which relates to NSA communications intelligence activities, including intelligence sources and methods, is also protected from release by statute and therefore is exempt from release based on the FOIA Exemption 3 statutes: 50 U.S.C. § 3605, 18 U.S.C. § 798, and 50 U.S.C. § 3024(i)(1).

81. Because DOJ OLC has withheld in full documents OLC 2, 3, 4, 6, and 8, and NSD Document 36 pursuant to FOIA Exemption 5, as described in more detail in the Declaration of Paul Colborn (“Colburn Declaration”) filed contemporaneously in connection with this motion, I have not attempted to determine whether and to what extent the classified information in those documents is reasonably segregable. In the event the Court determines that the information in these documents was not properly withheld in full under Exemption 5, NSA and other agencies will undertake a line-by-line review to segregate and release any non-exempt information in these documents.

82. NSA has conducted a line-by-line review of OLC 9, and all reasonably segregable, non-exempt portions of that document have been released. The limited information withheld is exempt from release under FOIA Exemptions 1 and 3. The information concerns NSA foreign intelligence activities, including information concerning communications intelligence targets, the scope of NSA collection against those targets, and specific collection and

processing methods employed. This information pertains to intelligence activities, intelligence sources or methods, or cryptology, or the vulnerabilities or capabilities of systems or projects relating to the national security and therefore meets the criteria for classification set forth in Sections 1.4(c) and 1.4(g) of EO 13526. Some of the withheld information concerns communications intelligence targets, the scope of NSA collection, and certain collection methods. The unauthorized disclosure of this information could be reasonably expected to cause serious damage to the national security for the reasons described in paragraph 80, *supra*. Accordingly, I have determined that this information is currently and properly classified at the SECRET level in accordance with EO 13526. Some of the other information withheld concerns particularly sensitive intelligence collection and processing techniques, the unauthorized disclosure of which could be reasonably expected to cause exceptionally grave damage to the national security. Once alerted to these collection and processing methods, adversaries could develop additional countermeasures to thwart collection and effective analysis of electronic communications. Such a reaction may result in a loss of information critical to the national security and defense of the United States. Therefore, I have determined that this information is currently and properly classified at the TOP SECRET level in accordance with EO 13526.

83. Finally, all of the classified information withheld from OLC 9 relates to NSA communications intelligence activities, including intelligence sources and methods. Therefore, the withheld information is also protected from release by statute, specifically: 50 U.S.C. § 3605, 18 U.S.C. § 798, and 50 U.S.C. § 3024(i)(1). *See supra*, ¶¶ 32-36. Therefore, the information withheld from that document is exempt from release under both FOIA Exemptions 1 and 3.

SEGREGABILITY

84. All of these documents have been reviewed for purposes of complying with FOIA's segregability provision, which requires the Government to release "any reasonably

segregable portion of a record” after proper application of the FOIA exemptions. 5 U.S.C. § 552(b). An intensive, line-by-line review of each document was performed,¹⁵ redactions were surgically applied to protect information exempted from release under the FOIA, and all reasonably segregable, non-exempt information has been released.

85. Further, in accordance with EO 13526 § 1.7(e), with respect to all of the information withheld under Exemption 1, it is my judgment that any information that, viewed in isolation, could be considered unclassified, is nonetheless classified in the context of this case because it can reasonably be expected to reveal (directly or by implication) classified national security information concerning the timing or nature of intelligence activities, sources, and methods when combined with other information that might be available to the public or adversaries of the United States. In these circumstances, the disclosure of even seemingly mundane information, such as document titles, when considered in conjunction with other publicly available information, could reasonably be expected to assist a sophisticated adversary in deducing particular intelligence activities or sources and methods, and possibly lead to the use of countermeasures that may deprive the United States of critical intelligence.

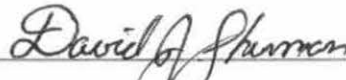
¹⁵ As noted above in paragraph 81, because all of NSA’s withholdings in OLC Documents 2, 3, 4, 6, and 8, and NSD Document 36 are subsumed within OLC’s Exemption 5 withholdings, NSA has not conducted a segregability review of these documents at this time. In the event the Court determines that information was not properly withheld under Exemption 5, NSA and other agencies will undertake a review to segregate and release any non-exempt information.

CONCLUSION

I declare under penalty of perjury that the foregoing is true and correct.

Executed at Fort Meade, Maryland, this 26th day of February, 2016, pursuant to 28 U.S.C.

§ 1746.

A handwritten signature in cursive script that reads "David J. Sherman". The signature is written in black ink and is positioned above a horizontal line.

Dr. David J. Sherman
Associate Director for Policy and Records,
National Security Agency

DOCID: 4052264

LEGAL DEPARTMENT



MAY 30 2013

May 13, 2013

BY USPS MAIL

Attn: Cindy Blacker
NSA FOIA Requester Service Center/DJ4
9800 Savage Road, Suite 6248
Ft. George G. Meade, MD 20744-6248

RE: FREEDOM OF INFORMATION ACT REQUEST

Dear Ms. Blacker,

The American Civil Liberties Union and the American Civil Liberties Union Foundation (together, the "ACLU") submit this request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, for access to documents relating to Executive Order 12,333, 3 C.F.R. 200 (1981 Comp.) ("EO 12,333"). Specifically, we request the following records¹:

1. Any records construing or interpreting the authority of the National Security Agency ("Agency") under Executive Order 12,333 or any regulations issued thereunder;
2. Any records describing the minimization procedures² used by the Agency with regard to both intelligence collection and intelligence interception conducted pursuant to the Agency's authority under EO 12,333 or any regulations issued thereunder; and
3. Any records describing the standards that must be satisfied for the "collection," "acquisition," or "interception" of communications, as the Agency defines these terms, pursuant to the Agency's authority under EO 12,333 or any regulations issued thereunder.

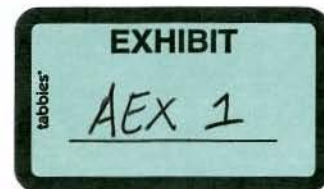
¹ Records include but are not limited to electronic records, letters, correspondence, tape recordings, notes, data, memoranda, reports, email, computer source and object code, technical manuals, technical specifications, legal opinions, policy statements, and any other materials.

² Minimization procedures include but are not limited to rules, policies, or procedures addressing the collection, interception, handling, use, retention, and destruction of information relating to U.S. persons that is acquired in the course of intelligence activities.

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET,
18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500
F/212.549.2651
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
SUSAN N. HERMAN PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR



DOCID: 4052264

Request for a Fee Limitation and Public Interest Fee Waiver

The ACLU requests a waiver of search and review fees because the requested records are not sought for commercial use and because the ACLU is a “representative of the news media.” 5 U.S.C. § 552(a)(4)(A)(ii)(II). Dissemination of information about actual or alleged government activity is a critical and substantial component of the ACLU’s mission and work. The ACLU disseminates this information to educate the public and promote the protection of civil liberties. Its regular means of disseminating and editorializing information obtained through FOIA requests include: a paper newsletter distributed to approximately 450,000 people; a bi-weekly electronic newsletter distributed to approximately 300,000 subscribers; published reports, books, pamphlets, and fact sheets; a widely read blog; heavily visited websites, including an accountability microsite, <http://www.aclu.org/accountability>; and a video series.

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET,
18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500
F/212.549.2651
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
SUSAN N. HERMAN PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

The ACLU therefore meets the statutory definition of a “representative of the news media” as an “entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience.” 5 U.S.C. § 552(a)(4)(A)(ii); *see also Nat’l Sec. Archive v. Dep’t of Def.*, 880 F.2d 1381, 1387 (D.C. Cir. 1989); *cf. Am. Civil Liberties Union v. Dep’t of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004) (finding non-profit public interest group to be “primarily engaged in disseminating information”). Indeed, the ACLU recently was held to be a “representative of the news media.” *Serv. Women’s Action Network v. Dep’t of Defense*, 888 F. Supp. 2d 282, 287-88 (D. Conn. 2012); *see also Am. Civil Liberties Union of Wash. v. Dep’t of Justice*, No. C09-0642RSL, 2011 WL 887731, at *10 (W.D. Wash. Mar. 10, 2011) (finding ACLU of Washington to be a “representative of the news media”), *reconsidered in part on other grounds*, 2011 WL 1900140 (W.D. Wash. May 19, 2011).

The ACLU also requests a waiver of all search, review, or duplication fees on the ground that disclosure of the requested information is in the public interest because: (1) it “is likely to contribute significantly to public understanding of the operations or activities of the government,” and (2) it “is not primarily in the commercial interest of the requester.” 5 U.S.C. § 552(a)(4)(A)(iii). This request clearly satisfies these criteria.

First, the requested material concerns “the operations or activities” of the Agency. E.O. 12,333 is “intended to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities and espionage conducted by foreign powers.” EO 12,333 § 2.2. It authorizes the intelligence community, including the Agency, to collect intelligence, and it sets forth certain limitations on intelligence-gathering activities relevant to civil liberties. In its brief in a

DOCID: 4052264

recent case before the Supreme Court of the United States, the Government emphasized its authority to conduct surveillance of Americans' foreign contacts abroad under Executive Order No. 12,333, without conforming to various statutory restrictions. Brief for Petitioners, *Clapper v. Amnesty Int'l USA*, No. 11-1025, 2012 WL 3090949, at *45 (U.S. 2012). How the Government actually does this, and whether it appropriately accommodates the constitutional rights of American citizens and residents whose communications are intercepted in the course of that surveillance, are matters of great significance.

Moreover, the requested materials will "contribute significantly to the public understanding" of the Agency's operations or activities. 5 U.S.C. § 552(a)(4)(A)(iii). Though the subject of foreign-intelligence collection is a matter of great public interest and concern, little information on how the American intelligence community construes the authority conferred by EO 12,333 and its implementing regulations is currently publicly available.

For example, in the *Clapper* brief described above, the government makes no argument beyond a handful of one-sentence assertions of its authority under EO 12,333. See Brief for Petitioners, *Clapper v. Amnesty Int'l USA*, No. 11-1025, 2012 WL 3090949 at *4, *33, *41, *45. Likewise, the publicly available administrative agency materials typically do little more than restate EO 12,333's limits on the intelligence community in slightly different ways or provide predictable definitions for terms left undefined in the executive order. See, e.g., Dep't of Def., DOD 5240 I-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons* § C2.3.12 (Dec. 1982); Nat'l Sec. Agency, *United States Signals Intelligence Directive* 18 (July 1993); Army Regulation 381-10, *U.S. Army Intelligence Procedures* § 2-2(l) (2007). Judicial treatments of EO 12,333 contribute equally little to the public understanding of the limits of intelligence-gathering powers under EO 12,333. See, e.g., *United States v. Marzook*, 435 F. Supp. 2d 778 (N.D. Ill. 2006); *United States v. Poindexter*, 727 F. Supp. 1470 (D.D.C. 1989); *United Presbyterian Church in the U.S.A. v. Reagan*, 738 F.2d 1375 (D.C. Cir. 1984).

For these reasons, we respectfully request that all fees related to the search, review, and duplication of the requested records be waived. If the search and review fees will not be waived, we ask that you contact us at the email address listed below should the estimated fees resulting from this request exceed \$100.

We request that responsive electronic records be provided electronically in their native file format, if possible. See 5 U.S.C. § 552(a)(3)(B). Alternatively, we request that the records be provided

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
375 BROAD STREET,
18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500
F/212.549.2651
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
SUSAN N. HERMAN PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

DOCID: 4052264

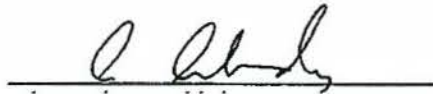
electronically in a text-searchable, static-image format (PDF), in the best image quality in the agency's possession, and in separate, Bates-stamped files.

We also request that you provide an estimated date on which you will finish processing this request. *See* 5 U.S.C. § 552(a)(7)(B).

If this FOIA request is denied in whole or in part, please provide the reasons for the denial, pursuant to 5 U.S.C. § 552(a)(6)(A)(i). In addition, please release all segregable portions of otherwise exempt material in accordance with 5 U.S.C. § 552(b). Furthermore, if any documents responsive to this request are classified, please identify those documents, including a date and document number where possible, so we may begin the process of requesting a Mandatory Declassification Review under the terms of Executive Order 13,526 (2010).

Thank you for your consideration of this request. If you have any questions or concerns, please do not hesitate to contact us at the email address listed below. Pursuant to 5 U.S.C. § 552(a)(6)(A)(i), we expect a response regarding this request within the twenty working-day statutory time limit.

Sincerely,



Alexander Abdo
Staff Attorney
National Security Project
American Civil Liberties Union

Phone: (212) 549-2517
Email: aabdo@aclu.org

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET,
18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500
F/212.549.2653
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
SUSAN N. HERMAN PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

DOCID: 4052264

US POSTAGE PITNEY BOWES
ZIP 10004 \$001.120
02 1W
0001363567 MAY 13 2013



FIRST CLASS

ATTN: CINDY BLACKER
NSA FOIA REQUESTER SERVICE CENTER / D34
9800 SAVAGE ROAD, SUITE 6248
FT. GEORGE G. MEADE, MD 20744-6248

OPEN BY CFSI
MAY 23 2013
INSPECTED BY CFSI



AMERICAN CIVIL
LIBERTIES UNION
NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400

DOCID: 4091714

Phillips, Pamela

From: Phillips, Pamela
Sent: Friday, June 28, 2013 10:30 AM
To: 'aabdo@aclu.org'
Cc: Phillips, Pamela
Subject: NSA FOIA Clarification

Mr. Abdo,

Thank you for speaking to me this morning about your FOIA request and helping us to scope it into a manageable search. We will continue to work with the organizations conducting the searches, and if we need any additional information to further clarify as we proceed, I will give you another call or email you. For the record, here is what we decided about your request today:

Case 70809 – for records construing or interpreting the authority of NSA under O.E. 12333; records describing the minimization procedures used by the Agency; records describing the standards that must be satisfied for collection, acquisition, or interception of communications

You agreed to limit the request to formally issued guidance (of which I mentioned various types, such as DoD Directions, NSA USSID, NSA Policies, various issuances relating to FISA, compliance training, and advisories). You agreed to omit guidance that simply reiterates or includes pieces and excerpts from the formal guidance. You also agreed that you are not seeking emails. Finally, you indicated that you would want any separate legal opinions that interpret the standards or define terms collection, acquisition, or interception to the extent that that opinion/interpretation is not included in the formal guidance.

Please let me know if I have mischaracterized or misunderstood our conversation in any way. You will be receiving a formal interim response from us soon with two previously released documents. Thanks again.

Pamela

Pamela N. Phillips
Chief, FOIA/PA Office (DJ4)
FOIA Public Liaison Officer
National Security Agency
(301) 688-6527
pnphill@nsa.gov





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

FOIA Case: 70809
1 July 2013

American Civil Liberties Union
ATTN: Mr. Alexander Abdo
National Office
125 Broad Street, 18th Fl.
New York, NY 10004-2400

Dear Mr. Abdo:

This is an initial response to your Freedom of Information Act (FOIA) request dated 13 May 2013, which was received by this office on 30 May 2013, for access to documents relating to Executive Order 12333, 3 C.F.R. 200, specially the following records:

1. Any records construing or interpreting the authority of the National Security Agency ("Agency") under Executive 12333 or any regulations issues thereunder;
2. Any records describing the minimization procedures used by the Agency with regard to both intelligence collection and intelligence interception conducted pursuant to the Agency's authority under EO 12333 or any regulations issued thereunder; and
3. Any records describing the standards that must be satisfied for the "collection," "acquisition," or "interception" of communications, as the Agency defines these terms, pursuant to the Agency's authority under EO 12333 or any regulations issued thereunder.

In a telephone conversation on 28 June 2013, you agreed to narrow your request to allow us to process it more quickly and to avoid search fees, since we have already begun processing several requests for similar information. You agree to limit your request (as relates to the above three items) to formally issued guidance, omitting emails and omitting guidance that reiterates or includes excerpts from the formal guidance. In addition, you indicated that you still desire any separate legal opinions that interpret the standards or define the terms in item 3 above, to the extent that it is not included in the formal guidance.



FOIA Case: 70809

Your request has been assigned Case Number 70809. This letter indicates that we have begun to process your request. There is certain information relating to this processing about which the FOIA and applicable Department of Defense (DoD) and NSA/CSS regulations require we inform you. For purposes of this request, you are considered an "all other" requester. However, as we already indicated, the search is being conducted in response to other requests, so there will be no search fees assessed for this request. In addition, we do not plan to charge the duplication fees for the responsive material for any of the requesters. Therefore, we have not addressed your request for a waiver of fees.

With this response, we enclose two documents (USSID 18 and NSA/CSS Policy 1-23, 81 pages in total) that were previously released under the FOIA. We are continuing our search for responsive materials and will contact you again as information becomes available.

Correspondence related to your request should include the case number assigned to your request, which is included in the first paragraph of this letter. Your letter should be addressed to National Security Agency, FOIA Office (DJ4), 9800 Savage Road STE 6248, Ft. George G. Meade, MD 20755-6248 or may be sent by facsimile to 443-479-3612. If sent by fax, it should be marked for the attention of the FOIA office. The telephone number of the FOIA office is 301-688-6527.

Sincerely,

A handwritten signature in cursive script, appearing to read "Pamela N. Phillips".

PAMELA N. PHILLIPS
Chief
FOIA/PA Office

Encls:
a/s

DOCID: 4091715

Phillips, Pamela

From: Alexander Abdo [aabdo@aclu.org]
Sent: Wednesday, August 21, 2013 11:04 PM
To: Phillips, Pamela
Subject: RE: NSA FOIA 70809

Thank you so much, Pamela.

We did in fact hear about the posting through a number of sources and have managed to download the documents from the website.

Alex

From: Phillips, Pamela [mailto:pnphill@nsa.gov]
Sent: Wednesday, August 21, 2013 4:40 PM
To: Alexander Abdo
Cc: Phillips, Pamela
Subject: NSA FOIA 70809

Mr. Abdo,

You may already be already aware, but my understanding is that the ODNI is going to post several documents this afternoon related to Section 702 were released today in a FOIA litigation case, some of which may also be responsive to your FOIA request to this agency for minimization procedures. They are to be posted to the ODNI website, and then later to the IContheRecord.tumblr.com website. We are continuing the processing of your request to this Agency and will respond further when documents are complete.

Pamela

Pamela N. Phillips
Chief, FOIA/PA Office (DJ4)
FOIA Public Liaison Officer
National Security Agency
(240) 373-1434
pnphill@nsa.gov
pnphill@nsa.smil.mil



NATIONAL SECURITY
PR
DOCID: 4086488



NOV 18 2013

November 8, 2013

BY UPS

NSA/CSS FOIA Appeal Authority (DJ4)
National Security Agency
9800 Savage Road, Suite 6248
Ft. George G. Meade, MD 20755-6248

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500
WWW.ACLU.ORG

RE: FREEDOM OF INFORMATION ACT APPEAL

Dear Sir or Madam,

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

The American Civil Liberties Union and the American Civil Liberties Union Foundation (together, the "ACLU") write to appeal from the constructive denial of their Freedom of Information Act request, submitted on May 13, 2013, for documents relating to Executive Order 12,333, 3 C.F.R. 200 (1981 Comp.) ("EO 12,333"). A copy of the request is attached here for reference. The ACLU received an acknowledgement of receipt dated July 1, 2013 in a letter signed by Pamela N. Philips. The request was assigned the following identification number: 70809.

Under the Freedom of Information Act, determinations about whether an agency will produce documents must be made within 20 business days. *See* 5 U.S.C. § 552(a)(6)(A)(i); 28 C.F.R. § 16.6(b). Where an agency cannot meet the statutory time limit due to unusual circumstances, the agency may extend the time limit by ten working days with written notice to the requester. 5 U.S.C. § 552(a)(6)(B). An agency denying a request in any respect must send the requester a signed letter including, among other things, a brief statement of the reasons for denial. 5 U.S.C. § 552(a)(6)(A)(i).

Because the twenty-day statutory time has elapsed without a substantive response, the National Security Agency has constructively failed to meet its legal obligation to disclose the information requested. By this appeal, we ask you to direct the timely disclosure of all records responsive to our request.



DOCID: 4086438

We thank you for your consideration of this appeal. Pursuant to 5 U.S.C. § 552(a)(6)(A)(ii), we expect a response regarding this appeal within twenty days. If you have any questions or concerns, please do not hesitate to contact me at the email address or telephone number indicated below.

Sincerely,



Alexander Abdo
Staff Attorney
National Security Project
American Civil Liberties Union
Phone: (212) 549-2517
Email: aabdo@aclu.org

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

DOCID: 4086438
LEGAL DEPARTMENT



May 13, 2013

BY USPS MAIL

Attn: Cindy Blacker
NSA FOIA Requester Service Center/DJ4
9800 Savage Road, Suite 6248
Ft. George G. Meade, MD 20744-6248

RE: FREEDOM OF INFORMATION ACT REQUEST

Dear Ms. Blacker,

The American Civil Liberties Union and the American Civil Liberties Union Foundation (together, the "ACLU") submit this request under the Freedom of Information Act ("FOIA"), 5 U.S.C. § 552, for access to documents relating to Executive Order 12,333, 3 C.F.R. 200 (1981 Comp.) ("EO 12,333"). Specifically, we request the following records¹:

1. Any records construing or interpreting the authority of the National Security Agency ("Agency") under Executive Order 12,333 or any regulations issued thereunder;
2. Any records describing the minimization procedures² used by the Agency with regard to both intelligence collection and intelligence interception conducted pursuant to the Agency's authority under EO 12,333 or any regulations issued thereunder; and
3. Any records describing the standards that must be satisfied for the "collection," "acquisition," or "interception" of communications, as the Agency defines these terms, pursuant to the Agency's authority under EO 12,333 or any regulations issued thereunder.

¹ Records include but are not limited to electronic records, letters, correspondence, tape recordings, notes, data, memoranda, reports, email, computer source and object code, technical manuals, technical specifications, legal opinions, policy statements, and any other materials.

² Minimization procedures include but are not limited to rules, policies, or procedures addressing the collection, interception, handling, use, retention, and destruction of information relating to U.S. persons that is acquired in the course of intelligence activities.

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET,
18TH FL.
NEW YORK, NY 10004-2400
T/212-549-2500
F/212-549-2651
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
SUSAN H. HERMAN PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

DOCID: 4086438

Request for a Fee Limitation and Public Interest Fee Waiver

The ACLU requests a waiver of search and review fees because the requested records are not sought for commercial use and because the ACLU is a “representative of the news media.” 5 U.S.C. § 552(a)(4)(A)(ii)(II). Dissemination of information about actual or alleged government activity is a critical and substantial component of the ACLU’s mission and work. The ACLU disseminates this information to educate the public and promote the protection of civil liberties. Its regular means of disseminating and editorializing information obtained through FOIA requests include: a paper newsletter distributed to approximately 450,000 people; a bi-weekly electronic newsletter distributed to approximately 300,000 subscribers; published reports, books, pamphlets, and fact sheets; a widely read blog; heavily visited websites, including an accountability microsite, <http://www.aclu.org/accountability>; and a video series.

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
115 BROAD STREET,
18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500
F/212.549.2651
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
SUSAN N. HERMAN PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

The ACLU therefore meets the statutory definition of a “representative of the news media” as an “entity that gathers information of potential interest to a segment of the public, uses its editorial skills to turn the raw materials into a distinct work, and distributes that work to an audience.” 5 U.S.C. § 552(a)(4)(A)(ii); *see also Nat’l Sec. Archive v. Dep’t of Def.*, 880 F.2d 1381, 1387 (D.C. Cir. 1989); *cf. Am. Civil Liberties Union v. Dep’t of Justice*, 321 F. Supp. 2d 24, 29 n.5 (D.D.C. 2004) (finding non-profit public interest group to be “‘primarily engaged in disseminating information’”). Indeed, the ACLU recently was held to be a “representative of the news media.” *Serv. Women’s Action Network v. Dep’t of Defense*, 888 F. Supp. 2d 282, 287-88 (D. Conn. 2012); *see also Am. Civil Liberties Union of Wash. v. Dep’t of Justice*, No. C09-0642RSL, 2011 WL 887731, at *10 (W.D. Wash. Mar. 10, 2011) (finding ACLU of Washington to be a “representative of the news media”), *reconsidered in part on other grounds*, 2011 WL 1900140 (W.D. Wash. May 19, 2011).

The ACLU also requests a waiver of all search, review, or duplication fees on the ground that disclosure of the requested information is in the public interest because: (1) it “is likely to contribute significantly to public understanding of the operations or activities of the government,” and (2) it “is not primarily in the commercial interest of the requester.” 5 U.S.C. § 552(a)(4)(A)(iii). This request clearly satisfies these criteria.

First, the requested material concerns “the operations or activities” of the Agency. E.O. 12,333 is “intended to enhance human and technical collection techniques, especially those undertaken abroad, and the acquisition of significant foreign intelligence, as well as the detection and countering of international terrorist activities and espionage conducted by foreign powers.” EO 12,333 § 2.2. It authorizes the intelligence community, including the Agency, to collect intelligence, and it sets forth certain limitations on intelligence-gathering activities relevant to civil liberties. In its brief in a

DOCID: 4086438

recent case before the Supreme Court of the United States, the Government emphasized its authority to conduct surveillance of Americans' foreign contacts abroad under Executive Order No. 12,333, without conforming to various statutory restrictions. Brief for Petitioners, *Clapper v. Amnesty Int'l USA*, No. 11-1025, 2012 WL 3090949, at *45 (U.S. 2012). How the Government actually does this, and whether it appropriately accommodates the constitutional rights of American citizens and residents whose communications are intercepted in the course of that surveillance, are matters of great significance.

Moreover, the requested materials will "contribute significantly to the public understanding" of the Agency's operations or activities. 5 U.S.C. § 552(a)(4)(A)(iii). Though the subject of foreign-intelligence collection is a matter of great public interest and concern, little information on how the American intelligence community construes the authority conferred by EO 12,333 and its implementing regulations is currently publicly available.

For example, in the *Clapper* brief described above, the government makes no argument beyond a handful of one-sentence assertions of its authority under EO 12,333. *See* Brief for Petitioners, *Clapper v. Amnesty Int'l USA*, No. 11-1025, 2012 WL 3090949 at *4, *33, *41, *45. Likewise, the publicly available administrative agency materials typically do little more than restate EO 12,333's limits on the intelligence community in slightly different ways or provide predictable definitions for terms left undefined in the executive order. *See, e.g.*, Dep't of Def., DOD 5240 1-R, *Procedures Governing the Activities of DOD Intelligence Components that Affect United States Persons* § C2.3.12 (Dec. 1982); Nat'l Sec. Agency, *United States Signals Intelligence Directive* 18 (July 1993); Army Regulation 381-10, *U.S. Army Intelligence Procedures* § 2-2(1) (2007). Judicial treatments of EO 12,333 contribute equally little to the public understanding of the limits of intelligence-gathering powers under EO 12,333. *See, e.g.*, *United States v. Marzook*, 435 F. Supp. 2d 778 (N.D. Ill. 2006); *United States v. Poindexter*, 727 F. Supp. 1470 (D.D.C. 1989); *United Presbyterian Church in the U.S.A. v. Reagan*, 738 F.2d 1375 (D.C. Cir. 1984).

For these reasons, we respectfully request that all fees related to the search, review, and duplication of the requested records be waived. If the search and review fees will not be waived, we ask that you contact us at the email address listed below should the estimated fees resulting from this request exceed \$100.

We request that responsive electronic records be provided electronically in their native file format, if possible. *See* 5 U.S.C. § 552(a)(3)(B). Alternatively, we request that the records be provided

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET,
18TH FL.
NEW YORK, NY 10004-2400
T/212-549-2500
F/212-549-2651
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
SUSAN N. HERMAN PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

DOCID: 4086438

electronically in a text-searchable, static-image format (PDF), in the best image quality in the agency's possession, and in separate, Bates-stamped files.

We also request that you provide an estimated date on which you will finish processing this request. *See* 5 U.S.C. § 552(a)(7)(B).

If this FOIA request is denied in whole or in part, please provide the reasons for the denial, pursuant to 5 U.S.C. § 552(a)(6)(A)(i). In addition, please release all segregable portions of otherwise exempt material in accordance with 5 U.S.C. § 552(b). Furthermore, if any documents responsive to this request are classified, please identify those documents, including a date and document number where possible, so we may begin the process of requesting a Mandatory Declassification Review under the terms of Executive Order 13,526 (2010).

Thank you for your consideration of this request. If you have any questions or concerns, please do not hesitate to contact us at the email address listed below. Pursuant to 5 U.S.C. § 552(a)(6)(A)(i), we expect a response regarding this request within the twenty working-day statutory time limit.

Sincerely,



Alexander Abdo
Staff Attorney
National Security Project
American Civil Liberties Union

Phone: (212) 549-2517
Email: aabdo@aclu.org

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET,
18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500
F/212.549.2651
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
SUSAN N. HERMAN PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

Extremely Urgent

This envelope is for use with the following services: **UPS Next Day Air***
UPS Worldwide Express*
UPS 2nd Day Air*

Visit ups.com* or call 1-800-PICK-UPS* (1-800-742-5877) to schedule a pickup or find a drop off location near you.

Insert shipping documents under window from the top.

Domestic Shipments
* To qualify for the Letter rate, UPS Express Envelopes may only contain one letter and must be addressed to a U.S. residential address.

Do not use this envelope for:

Standard
Select*
2nd Day Air*
Expedited*

ALEX ANHO 2125 492500 JUL17 125 BROADWAY NEW YORK NY 10004	SHIP TO: NATIONAL SECURITY AGENCY NSN/CSS FOIA APPL. AUTHORITY (DIA) SUITE 6248 9800 SAVAGE ROAD FORT GEORGE G MEADE MD 20755-6248	0.0 LBS LTR 1 OF 1	MD 207 9-37 	UPS NEXT DAY AIR SAVER 1P TRACKING #: 1Z 149 080 13 9399 5262 		BILLING: 1P/P Department: National Security Class/Accounting Code: No Ltr 48 13 9 13 13 
---	--	-----------------------	--	---	---	---

OPEN BY CFSI
 NOV 1 2 2013
INSPECTED BY CFSI

https://www.campusship.ups.com/cship/create?ActionOriginPair=default__PrintWindowPage&key=labelWindow&t...

DOCID: 4086438
100% Recycled fiber
80% Post-Consumer

International Shipping Notice: Carriage hereunder may be subject to the rules relating to liability and other terms and conditions established by the Convention for the Unification of Certain Rules Relating to International Carriage by Air (The "Chicago Convention") and to the Convention on the Contract for the International Carriage of Goods by Road (the "CMR Convention"). These commodities, technology or software were exported from the U.S. in accordance with the Export Administration Regulations. Diversion outside the U.S. is prohibited.

DOCID: 4091291

Phillips, Pamela

From: Phillips, Pamela
Sent: Monday, November 18, 2013 4:00 PM
To: 'aabdo@aclu.org'
Cc: Phillips, Pamela
Subject: NSA FOIA Release of USSID SP0018 for 70809 (ACLU)

Mr. Abdo,

Attached is a follow-up response to your FOIA request 70809 and the updated version of USSID SP0018 (and Annex J). The ODNI is making another release of additional documents (nearly 2000 pages) relating to collection under Section 501 later today. You will be able to find it at www.dni.gov, as well as the DNI's public website IContheRecord.tumblr.com. Once you've had the opportunity to look through it, please let us know whether that material satisfies your FOIA request, or whether you require additional information from us. We will also send you the hard copy of your response and the documents unless you indicate that this email is sufficient.



Abdo 70809.pdf



USSID SP0018.pdf



USSID SP0018
Annex J.pdf

Respectfully,
Pamela

Pamela N. Phillips
Chief, FOIA/PA Office (DJ4)
FOIA Public Liaison Officer
National Security Agency
(240) 373-1434
pnphill@nsa.gov
pnphill@nsa.smil.mil





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

FOIA Case: 70809A
18 November 2013

American Civil Liberties Union
ATTN: Mr. Alexander Abdo
National Office
125 Broad Street, 18th Fl.
New York, NY 10004-2400

Dear Mr. Abdo:

This further responds to your Freedom of Information Act (FOIA) request dated 13 May 2013 for access to documents relating to Executive Order (EO) 12333, 3 C.F.R. 200, specifically the following records:

1. Any records construing or interpreting the authority of the National Security Agency ("Agency") under EO 12333 or any regulations issues thereunder;
2. Any records describing the minimization procedures used by the Agency with regard to both intelligence collection and intelligence interception conducted pursuant to the Agency's authority under EO 12333 or any regulations issued thereunder; and
3. Any records describing the standards that must be satisfied for the "collection," "acquisition," or "interception" of communications, as the Agency defines these terms, pursuant to the Agency's authority under EO 12333 or any regulations issued thereunder.

You agreed to narrow your request (as relates to the above three items) to formally issued guidance, omitting emails and omitting guidance that reiterates or includes excerpts from the formal guidance. In addition, you indicated that you still desire any separate legal opinions that interpret the standards or define the terms in item 3 above, to the extent that it is not included in the formal guidance.

Two additional documents responsive to your request (USSID SP0018 and Annex J) have been processed under the FOIA and are enclosed. Certain information, however, has been deleted from the enclosures.



FOIA Case: 70809A

Some of the information deleted from the documents was found to be currently and properly classified in accordance with Executive Order 13526. This information meets the criteria for classification as set forth in Subparagraphs (c) and/or (d) of Section 1.4 and remains classified SECRET as provided in Section 1.2 of the Executive Order. The information is classified because its disclosure could reasonably be expected to cause serious damage to the national security. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)).

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in these documents. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 3024(i) (formerly Title 50 U.S. Code 403-1(i)); and Section 6, Public Law 86-36 (50 U.S. Code 3605, formerly 50 U.S. Code 402 note).

The Initial Denial Authority for NSA information is the Associate Director for Policy and Records, David J. Sherman. Since these deletions may be construed as a partial denial of your request, you are hereby advised of this Agency's appeal procedures. Any person denied access to information may file an appeal to the NSA/CSS Freedom of Information Act Appeal Authority. The appeal must be postmarked no later than 60 calendar days from the date of the initial denial letter. The appeal shall be in writing addressed to the NSA/CSS FOIA Appeal Authority (DJ4), National Security Agency, 9800 Savage Road STE 6248, Fort George G. Meade, MD 20755-6248. The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes release of the information is required. The NSA/CSS Appeal Authority will endeavor to respond to the appeal within 20 working days after receipt, absent any unusual circumstances.

The State Department has also asked that we protect information pursuant to 5 U.S.C. 552(b)(1). We will coordinate any appeal of the denial of that information with the State Department.

Review of additional documents responsive to your request continues; they will be provided to you as they are completed. In addition, documents related to NSA collection activities and procedures continue to be released in litigation on behalf of the Intelligence Community (IC) by the Office of the Director of National Intelligence (ODNI). You will find those documents posted

FOIA Case: 70809A

on the ODNI web page, as well as on IC on the Record
(IContheRecord.tumblr.com).

Sincerely,

A handwritten signature in black ink, appearing to read "Pamela N. Phillips". The signature is written in a cursive style with a large initial "P".

PAMELA N. PHILLIPS
Chief
FOIA/PA Office

Encls:
a/s



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

Case No: 70809 / Appeal No: 3866
22 November 2013

American Civil Liberties Union
ATTN: Mr. Alexander Abdo
National Office
125 Broad Street, 18th Fl.
New York, NY 10004-2400

Dear Mr. Abdo:

This acknowledges receipt of your correspondence, dated 8 November 2013, appealing the National Security Agency's (NSA's) denial of your Freedom of Information Act (FOIA) request of 13 May 2013 for access to documents relating to Executive Order (EO) 12333, specifically the following records:

1. Any records construing or interpreting the authority of the National Security Agency ("Agency") under EO 12333 or any regulations issues thereunder;
2. Any records describing the minimization procedures used by the Agency with regard to both intelligence collection and intelligence interception conducted pursuant to the Agency's authority under EO 12333 or any regulations issued thereunder; and
3. Any records describing the standards that must be satisfied for the "collection," "acquisition," or "interception" of communications, as the Agency defines these terms, pursuant to the Agency's authority under EO 12333 or any regulations issued thereunder.

Your appeal was received by the NSA Office of Associate General Counsel (Litigation) on 19 November 2013 and has been assigned Appeal Number 3866.

Please be advised that appeals are processed in the order in which they are received, on a first-in, first-out basis. At this time, there are a large number of appeals ahead of yours in our queue. We will begin to process your appeal and will respond to you again as soon as we are able. We appreciate your understanding in this matter.

Correspondence related to your request should include the case and appeal numbers assigned to your request and be addressed to the National Security Agency, Office of Associate General Counsel (Litigation), FOIA/PA Appeals, 9800 Savage Road, Suite 6278, Fort George G. Meade, MD 20755-6278; or it may be sent via facsimile to 443-479-1111. If sent by fax, it should be marked for the attention of "FOIA Appeals." For inquiries regarding the status of your appeal, please contact this office via email at FOIA_Appeal_Status@nsa.gov.

Sincerely,

A handwritten signature in cursive script, appearing to read "Brian C.", written in dark ink.

Brian C.
FOIA/PA Appeals Program Manager
Office of Associate General Counsel (Litigation)



DOJ/DIGITAL SECURITY PROJECT 4093210



read
JAN 16 2014

January 9, 2014

VIA UPS

NSA/CSS FOIA Appeal Authority (DJ4)
National Security Agency
9800 Savage Road STE 6248
Ft. George G. Meade, MD 20755-6248

RE: FREEDOM OF INFORMATION ACT APPEAL
FOIA REQUEST NO. 70809

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212 549.2500
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

Dear Sir or Madam:

The American Civil Liberties Union and American Civil Liberties Union Foundation (collectively, "ACLU") write to appeal from the response of the National Security Agency/Central Security Service ("NSA") to FOIA request number 70809, attached hereto as Exhibit A. In that request, the ACLU seeks the following records:

1. Any records construing or interpreting the authority of the National Security Agency ("Agency") under Executive Order 12,333 ("EO 12,333") or any regulations issued thereunder;
2. Any records describing the minimization procedures used by the Agency with regard to both intelligence collection and intelligence interception conducted pursuant to the Agency's authority under EO 12,333 or any regulations issued thereunder; and
3. Any records describing the standards that must be satisfied for the "collection," "acquisition," or "interception" of communications, as the Agency defines these terms, pursuant to the Agency's authority under EO 12,333 or any regulations issued thereunder.

By letter dated July 1, 2013, attached hereto as Exhibit B, Pamela Phillips, Chief of the FOIA/PA Office enclosed two documents responsive to the request, specifically USSID 18 (dated July 27, 1993) and NSA/CSS Policy 1-23 (dated Mar. 11, 2004). Those documents had previously been released to the public under the FOIA and were produced to the ACLU with extensive redactions, each of which was annotated with one or more of the following asserted grounds for withholding: FOIA Exemption 1, FOIA Exemption 3 and three particular withholding statutes, 50 U.S.C. § 403, 18 U.S.C. § 798, and Pub. L. No. 86-36.

EXHIBIT

tabbles

AEX9

DOCID: 4093210

The letter indicated that searches for records responsive to the ACLU's request were ongoing. The letter did not indicate that it was a final decision, and did not indicate that it was subject to appeal.

In a second letter, dated November 18, 2013, and attached hereto as Exhibit C, Ms. Phillips produced two additional documents responsive to the request, specifically USSID SP0018 (dated Jan. 25, 2011), and Annex J (dated Apr. 24, 1986). These documents were also produced with extensive redactions pursuant to the FOIA Exemption 1 and 3, and the following specific withholding statutes: 50 U.S.C. § 3024(i), 18 U.S.C. § 798, and Pub. L. No. 86-36 § 6. The letter indicated that some of the Exemption 1 redactions had been made pursuant to a request from the Department of State.

The November 18 letter further indicated that the NSA continued to review additional records responsive to the ACLU's request, but provided no timeline for issuance of a complete response to the request. The letter indicated that the redactions "may be construed as a partial denial of [the ACLU's] request," and advised the ACLU of the NSA's appeal procedures.

This letter therefore timely appeals the NSA's decision to redact information from the four documents released to date.¹ FOIA enacts into law a strong policy favoring disclosure of agency records. Records may be withheld only if the agency can demonstrate that certain records, or portions thereof, come within one or more narrowly construed exemptions. *See Mead Data Cent., Inc. v. U.S. Dep't of Air Force*, 566 F.2d 242, 259 (D.C. Cir. 1977) ("The exemptions from the mandatory disclosure requirement of the FOIA are both narrowly drafted and narrowly construed in order to counterbalance the self-protective instincts of the bureaucracy which, like any organization, would prefer to operate under the relatively comforting gaze of only its own members rather than the more revealing "sunlight" of public scrutiny.").

Here, the NSA has failed to adequately justify any of the redactions from the four documents in question, offering only the conclusory assertion that various asserted grounds for withholding apply to the redactions. The NSA has not

¹ The ACLU filed suit against the NSA on December 30, 2013, with respect to the FOIA request at issue in this appeal. *See ACLU v. NSA*, No. 13-cv-9198 (S.D.N.Y. filed Dec. 30, 2013). That lawsuit challenges the NSA's failure to timely produce all responsive records, and its failure to adjudicate and grant the ACLU's request for a waiver and limitation of fees. To the extent that the NSA's decision to redact the four documents released to date constitute agency decisions subject to administrative appeal, the ACLU files this appeal in order to exhaust administrative remedies on that issue. In the event that this administrative appeal is unsuccessful, or is not timely decided, the ACLU may take steps necessary to obtain judicial review of the lawfulness of the NSA's redactions in the four documents at issue.

DOCID: 4093210

provided any “detailed” or “specific” justifications for why any of the withheld information properly comes within an exemption, as it is required to do. *See generally Vaughn v. Rosen*, 484 F.2d 820 (1973) (“[C]ourts will simply no longer accept conclusory and generalized allegations of exemptions.”); *Mead Data Central, Inc. v. U.S. Dep’t of the Air Force*, 566 F.2d 242, 251 (D.C. Cir. 1977) (“[T]he objective of the *Vaughn* requirements, to permit the requesting party to present its case effectively, is equally applicable to proceedings within the agency.”).

Each of the grounds for withholding asserted by the NSA—FOIA Exemption 1 and various withholding statutes under FOIA Exemption 3—require the agency to demonstrate that the information redacted meets particular criteria. Thus, for instance, in order to withhold information pursuant to Exemption 1, the NSA must demonstrate that each item of redacted information is properly classified pursuant to Executive Order 13,526, which requires that information (1) is classified by an original classification authority, (2) is owned, produced, or controlled by the U.S. government, (3) pertains to one or more of eight classifiable subject matters specified in section 1.4 of the executive order, and (4) that unauthorized disclosure reasonably could be expected to result in damage to national security. Exec. Order No. 13,526 (Dec. 29, 2009). The NSA has not attempted to explain why any of these four requirements are met with respect to any of the many redactions in the four documents at issue. Instead, the NSA’s letter simply recites the requirements of the Executive Order and asserts that they have been met. *See Exhibit B*. This is plainly inadequate and does not suffice to overcome FOIA’s strong presumption in favor of disclosure.

The NSA has similarly failed to justify its invocation of the various withholding statutes it relies on under Exemption 3. For instance, 50 U.S.C. § 3024(i) (and its predecessor, 50 U.S.C. § 403-1), covers only “intelligence sources and methods,” yet the NSA has provided no description or other explanation of the withheld information to indicate that the redacted information would, if disclosed, reveal any intelligence source or method.

In addition, the NSA may not redact information from the documents that it has elsewhere disclosed to the public through official channels. *See Hudson River Sloop Clearwater, Inc. v. Dep’t of the Navy*, 891 F.2d 414, 421 (2d Cir. 1989). Moreover, where information has come into the public domain, whether through official channels or otherwise, agencies seeking to withhold that information bear a heightened burden to justify redactions because they must demonstrate that disclosure would somehow cause harm to national security even though the information has already become public. *See Washington Post v. U.S. Dep’t of Defense*, 766 F. Supp. 1, 9–11 (D.D.C. 1991).

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

DOCID: 4093210

In recent months, the NSA has officially disclosed a significant amount of information about its intelligence activities.² Moreover, the press has reported on many other aspects of the NSA's activities, and those reports have been addressed by various government officials, including those at the NSA.³ The NSA's letters accompanying the redacted documents in question fail to provide any indication that information redacted from those documents has not elsewhere been officially acknowledged. Nor do the letters provide any justification for withholding information in light of the extensive information now in the public record.

Because the NSA has failed to justify any of its redactions, we ask that the documents in question be released without redactions, or else that the ACLU be provided with an adequate justification for any remaining redactions. In accordance with the FOIA, we expect a response within 20 working days. Please send any correspondence to the address indicated below.

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION

Sincerely,



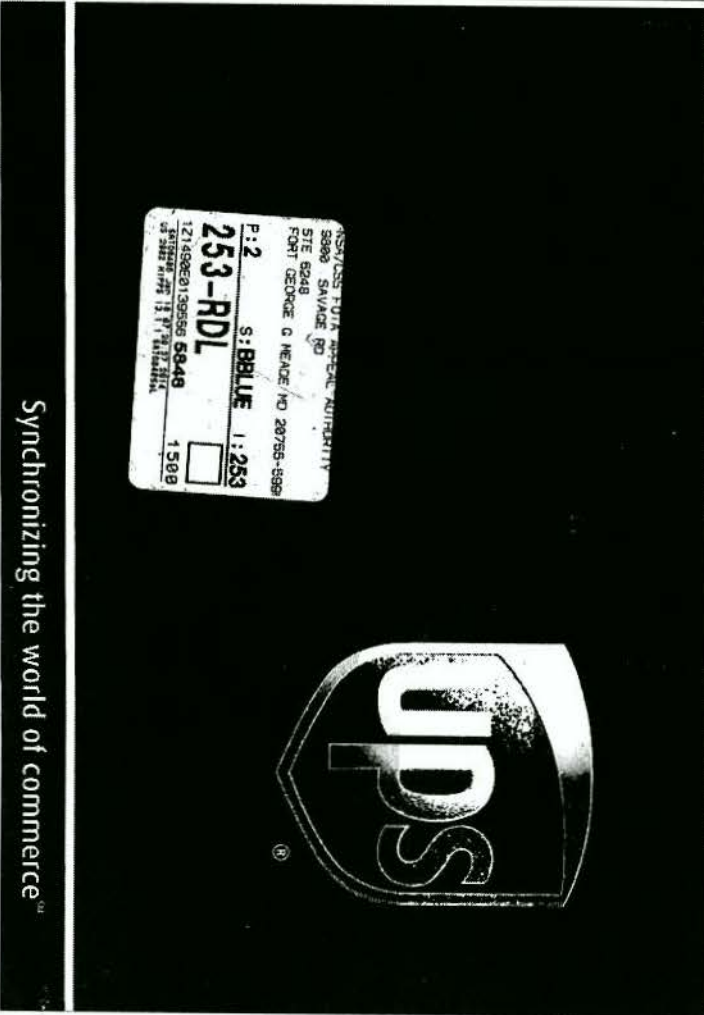
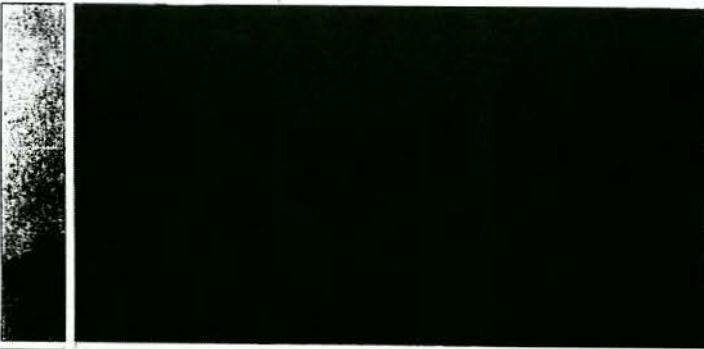
Alexander Abdo
Staff Attorney
American Civil Liberties Union
Foundation
125 Broad Street, 18th Floor
New York, NY 10004
Tel: (212) 549-2517
Fax: (212) 549-2629
Email: aabdo@aclu.org

² See, e.g., Office of Director of Nat'l Intelligence, IC on the Record, icontherecord.tumblr.com; *60 Minutes: Inside the NSA* (CBS News broadcast Dec. 16, 2013).

³ See generally, *Timeline of Edward Snowden Revelations*, Al Jazeera America (last visited Jan. 7, 2014) (compiling and providing links to press reports since June 2013 regarding the NSA's activities), <http://america.aljazeera.com/articles/multimedia/timeline-edward-snowden-revelations.html>.

DOCID: 4093210

Express Envelope



121458260139556 5949
 253-RDL
 P:2 S:BRILLE 1:253
 1508
 121458260139556 5949
 253-RDL
 P:2 S:BRILLE 1:253
 1508



Synchronizing the world of commerce™



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

Case No: 70809 / Appeal No: 3897
24 January 2014

American Civil Liberties Union
ATTN: Mr. Alexander Abdo
National Office
125 Broad Street, 18th Fl.
New York, NY 10004-2400

Dear Mr. Abdo:

This acknowledges receipt of your correspondence, dated 9 January 2014, appealing the National Security Agency's (NSA's) withholdings in four documents that were provided to you in response to your Freedom of Information Act (FOIA) request of 13 May 2013 for access to documents relating to Executive Order (EO) 12333, specifically the following records:

1. Any records construing or interpreting the authority of the National Security Agency ("Agency") under EO 12333 or any regulations issues thereunder;
2. Any records describing the minimization procedures used by the Agency with regard to both intelligence collection and intelligence interception conducted pursuant to the Agency's authority under EO 12333 or any regulations issued thereunder; and
3. Any records describing the standards that must be satisfied for the "collection," "acquisition," or "interception" of communications, as the Agency defines these terms, pursuant to the Agency's authority under EO 12333 or any regulations issued thereunder.

Your appeal was received by the NSA Office of Associate General Counsel (Litigation) on 17 January 2014 and has been assigned Appeal Number 3897.

Please be advised that appeals are processed in the order in which they are received, on a first-in, first-out basis. At this time, there are a large number of appeals ahead of yours in our queue. We will begin to process your appeal and will respond to you again as soon as we are able. We appreciate your understanding in this matter.

Correspondence related to your request should include the case and appeal numbers assigned to your request and be addressed to the National Security Agency, Office of Associate General Counsel (Litigation), FOIA/PA Appeals, 9800 Savage Road, Suite 6278, Fort George G. Meade, MD 20755-6278; or it may be sent via facsimile to 443-479-1111. If sent by fax, it should be marked for the attention of "FOIA Appeals." For inquiries regarding the status of your appeal, please contact this office via email at FOIA_Appeal_Status@nsa.gov.

Sincerely,

A handwritten signature in black ink, appearing to read "Brian C.", written in a cursive style.

Brian C.

FOIA/PA Appeals Program Manager
Office of Associate General Counsel (Litigation)





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

FOIA Case: 70809B
1 May 2014

ATTN ALEXANDER ABDO
AMERICAN CIVIL LIBERTIES UNION
NATIONAL OFFICE
125 BROAD ST 18TH FL
NEW YORK NY 10004-2400

Dear Mr. Abdo:

This is our final response to your Freedom of Information Act (FOIA) request of 13 May 2013, which was received by this office on 30 May 2013, for access to documents relating to Executive Order 12333, 3 C.F.R. 200, specifically the following records:

1. Any records construing or interpreting the authority of the National Security Agency ("Agency") under Executive 12333 or any regulations issued thereunder;
2. Any records describing the minimization procedures used by the Agency with regard to both intelligence collection and intelligence interception conducted pursuant to the Agency's authority under EO 12333 or any regulations issued thereunder; and
3. Any records describing the standards that must be satisfied for the "collection," "acquisition," or "interception" of communications, as the Agency defines these terms, pursuant to the Agency's authority under EO 12333 or any regulations issued thereunder.

A copy of your request is enclosed. Per a phone conversation on 28 June 2013, you agreed to narrow your request to formally issued guidance. Your request has been processed under the FOIA, and a search of our records identified several items that are responsive to your request.

In our initial written response to you, dated 1 July 2013, we provided a copy of two documents that had been previously released, USSID 18 and NSA/CSS Policy 1-23, and informed you that we were continuing to work on your request. We notified you via email on 21 August 2013 of the impending



FOIA Case: 70809B

ODNI release of documents to the ODNI website and later to the "IcontheRecord" Tumblr website, indicating that some of the documents may be responsive to your request. You responded on 21 August 2013 that you were aware of the posting and had downloaded documents from the website. In our next written response to you, dated 18 November 2013, we provided a copy of USSID SP0018 and USSID SP0018 Annex J. Also on 18 November 2013, we sent you an email with these two files attached, and informed you of another impending ODNI document release of nearly 2000 pages, and asked you to inform us whether that material satisfied your request. We did not receive a response, and we continued to process your request.

We have completed our review, and determined that all but one document responsive to this request has been released by the ODNI. These documents can be found at www.icontherecord.tumblr.com. The final document is enclosed. Certain information, however, has been deleted from the enclosure.

Some of the information deleted from the document was found to be currently and properly classified in accordance with Executive Order 13526. This information meets the criteria for classification as set forth in Subparagraph (c) of Section 1.4 and remains classified TOP SECRET as provided in Section 1.2 of the Executive Order. The information is classified because its disclosure could reasonably be expected to cause exceptionally grave damage to the national security. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)).

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in this document. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA which provides for the withholding of information specifically protected from disclosure by statute. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 3024(i); and Section 6, Public Law 86-36 (50 U.S. Code 3605).

The Initial Denial Authority for NSA information is the Associate Director for Policy and Records, David J. Sherman. Since these deletions may be construed as a partial denial of your request, you are hereby advised of this Agency's appeal procedures. Any person denied access to information may file an appeal to the NSA/CSS Freedom of Information Act Appeal Authority. The appeal must be postmarked no later than 60 calendar days from the date of the initial denial letter. The appeal shall be in writing addressed to the NSA/CSS

FOIA Case: 70809B

FOIA Appeal Authority (DJ4), National Security Agency, 9800 Savage Road STE 6248, Fort George G. Meade, MD 20755-6248. The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes release of the information is required. The NSA/CSS Appeal Authority will endeavor to respond to the appeal within 20 working days after receipt, absent any unusual circumstances.

Sincerely,

A handwritten signature in black ink, appearing to read "Pamela N. Phillips". The signature is written in a cursive, flowing style.

PAMELA N. PHILLIPS
Chief
FOIA/PA Office

Encls:
a/s

Jones, A.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

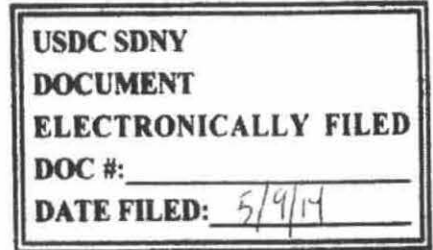
AMERICAN CIVIL LIBERTIES UNION, and
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY,
CENTRAL INTELLIGENCE AGENCY,
DEPARTMENT OF DEFENSE,
DEPARTMENT OF JUSTICE, and
DEPARTMENT OF STATE,

Defendants.



13 Civ. 9198 (AT)

STIPULATION AND ORDER REGARDING DOCUMENT SEARCHES

WHEREAS, on May 13, 2013, Plaintiffs the American Civil Liberties Union and the American Civil Liberties Union Foundation (collectively, "Plaintiffs") made requests (the "Requests") pursuant to the Freedom of Information Act ("FOIA") to various government agencies, including, as relevant here, the National Security Agency ("NSA"), the Central Intelligence Agency ("CIA"), the Defense Intelligence Agency ("DIA"), the Department of Justice's Office of Legal Counsel ("OLC"), the Department of Justice's National Security Division ("NSD"), the Federal Bureau of Investigation ("FBI") and the Department of State ("State") (collectively, the "Agencies") relating to the Agencies' respective authorities pursuant to Executive Order ("EO") 12,333, and activities undertaken pursuant to those authorities;

WHEREAS, over the course of the administrative processing of Plaintiffs' FOIA requests, Plaintiffs came to agreements with NSA and OLC regarding the scope of searches that



these agencies would perform in full resolution of the relevant Requests, and these agencies thereafter began searching for and processing documents based on these agreements:

WHEREAS, on December 30, 2013, Plaintiffs filed a complaint in the instant action against the NSA, CIA, the Department of Defense (“DoD”), the Department of Justice (“DOJ”), and State (collectively, the “Defendants,” and together with Plaintiffs, the “Parties”) seeking judicial assistance in securing the Agencies’ responses to their Requests;

WHEREAS, on February 18, 2014, Plaintiffs filed an amended complaint in this action;

WHEREAS, on March 3, 2014, Defendants answered the amended complaint;

AND WHEREAS, the Parties have engaged in discussions in an attempt to reach agreement on the scope of searches that the Agencies will undertake in response to the Requests.

NOW, THEREFORE, it is hereby STIPULATED and AGREED between the Parties as follows:

1. The searches the Agencies agree to undertake that are described herein are deemed to fulfill in full the Agencies’ search obligations under the respective Requests.
2. OLC will continue to search for and process only those documents encompassed by the agreement it reached with Plaintiffs during the administrative processing of the relevant Request.
3. NSA, CIA, DIA, FBI, and State will search for and process only the following categories of documents:
 - a. Any formal regulations or policies relating to that Agency’s authority under EO 12,333 to undertake “Electronic Surveillance” (as that term is defined in EO 12,333) that implicates “United States Persons” (as that term is defined in EO 12,333), including regulations or policies relating to that Agency’s

acquisition, retention, dissemination, or use of information or communications to, from, or about United States Persons under such authority.¹

- b. Any document that officially authorizes or modifies under EO 12,333 that Agency's use of specific programs, techniques, or types of Electronic Surveillance that implicate United States Persons, or documents that adopt or modify official rules or procedures for the Agency's acquisition, retention, dissemination, or use of information or communications to, from, or about United States persons under such authority generally or in the context of particular programs, techniques, or types of Electronic Surveillance.
- c. Any formal legal opinions addressing that Agency's authority under EO 12,333 to undertake specific programs, techniques, or types of Electronic Surveillance that implicates United States Persons, including formal legal opinions relating to that Agency's acquisition, retention, dissemination, or use of information or communications to, from, or about United States Persons under such authority generally or in the context of particular programs, techniques, or types of Electronic Surveillance.
- d. Any formal training materials or reference materials (such as handbooks, presentations, or manuals) that expound on or explain how that Agency implements its authority under EO 12,333 to undertake Electronic Surveillance that implicates United States Persons, including its acquisition,

¹ For purposes of this Stipulation, surveillance that "implicates" United States Persons means surveillance that is reasonably believed to involve the interception, acquisition, scanning, or collection of information or communications to, from, or about a United States Person or persons even if the target of such surveillance is not a United States Person.

retention, dissemination, or use of information or communications to, from, or about United States Persons under such authority.

- e. Any formal reports relating to Electronic Surveillance under EO 12,333 implicating United States Persons, one of whose sections or subsections is devoted to (1) the Agency's compliance, in undertaking such surveillance, with EO 12,333, its implementing regulations, the Foreign Intelligence Surveillance Act, or the Fourth Amendment; or (2) the Agency's interception, acquisition, scanning, or collection of the communications of United States Persons, whether "incidental" or otherwise, in undertaking such surveillance; and that are or were:

- i. Authored by the Agency's inspector general or the functional equivalent thereof;
- ii. Submitted by the Agency to Congress, the Office of the Director of National Intelligence, the Attorney General, or the Deputy Attorney General; or
- iii. Maintained by the office of the Agency's director or head.

4. NSD will search for and process all documents responsive to the original FOIA Request submitted to it by Plaintiffs.

5. If, in the course of searching for the records described in Paragraphs 3 or 4, an Agency discovers responsive records of other Agencies, it shall refer those documents to the originating Agency for processing.

6. With respect to the categories of documents described in Paragraph 3(b) and 3(e)(ii) above, CIA will search for such materials only in the offices of the Director, Deputy

Director, and Executive Director of the CIA, as well as materials maintained at the directorate level. With respect to the categories of documents described in Paragraph 3(c) above, CIA will search for such materials only in the particular division of CIA's Office of General Counsel that is responsible for providing legal advice on complex or novel questions (the "CIA OGC Division"). With respect to the categories of documents described in Paragraph 3(d) above, CIA will search for such materials created by the CIA OGC Division or created or maintained at the directorate level.

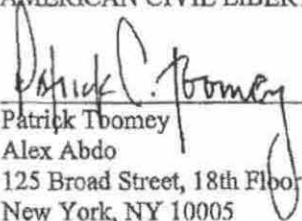
7. Date limitations.
 - a. Paragraphs 3(a)–(c). With respect to the categories of documents described in Paragraphs 3(a)–(c) above, each Agency will search for and process only documents that are currently in use or effect, or that were created or modified on or after September 11, 2001.
 - b. Paragraph 3(d). With respect to the categories of documents described in Paragraph 3(d) above, each Agency will search for and process only documents that are currently in use or effect.
 - c. Paragraph 3(e). With respect to the categories of documents described in Paragraph 3(e) above, each Agency will initially search for and process only documents created or modified on or after September 11, 2001; after the completion of the Agency's production of these documents, the parties agree to continue their discussions regarding whether searches for documents created before September 11, 2001 will be undertaken, including whether conducting such searches would be unduly burdensome to the Agencies.

8. Nothing in this Stipulation and Order, including the fact of its entry, should be taken as a concession by Defendants that Plaintiffs have "substantially prevailed" in this action in whole or in part, as that term is used in 5 U.S.C. § 552(a)(4)(E).

Dated: New York, New York
May 9, 2014

AMERICAN CIVIL LIBERTIES UNION

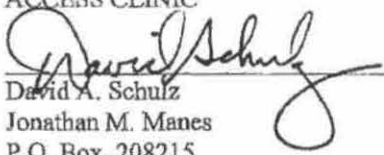
By:


Patrick Toomey
Alex Abdo
125 Broad Street, 18th Floor
New York, NY 10005
Phone: (212) 549-2500
Fax: (212) 549-2654
Email: ptoomey@aclu.org

Dated: New Haven, Connecticut
May 9, 2014

MEDIA FREEDOM AND INFORMATION
ACCESS CLINIC

By:

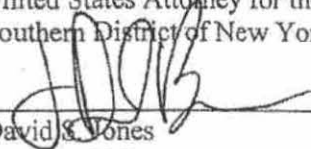

David A. Schulz
Jonathan M. Manes
P.O. Box. 208215
New Haven, CT 06520
(212) 850-6103

Counsel for Plaintiffs

Dated: New York, New York
May 9, 2014

PREET BHARARA
United States Attorney for the
Southern District of New York

By:



David S. Jones
Jean-David Barnea
Assistant United States Attorneys
86 Chambers Street, Third Floor
New York, New York 10007
Telephone: (212) 637-2739/2679
Facsimile: (212) 637-2730
E-mail: david.jones6@usdoj.gov
jean-david.barnea@usdoj.gov

Counsel for Defendants

SO ORDERED:



ANALISA TORRES
United States District Judge

May 9, 2014

Date

4n
8

UNCLASSIFIED

American Civil Liberties Union et. al. v. National Security Agency et. al.

Civil Action No. 13-9198 (AT)
 U.S. District Court
 Southern District of New York

(U) Vaughn Index

(U) This index contains a description of the 20 records released in full, denied in full or released in part by the NSA that have been included in Defendants' litigation sample. The disposition of the document(s) is noted with "RIF" which means released in full, "RIP" which means released-in-part, and "DIF" which means denied in full.

Documents Challenged by ACLU							
Doc No.	Doc. Date	Title	Description	Disposition	Exemption(s)	Pages	Production Date
5	05 May 10	SID Management Directive (SMD) 432, Procedural Guidelines for SIGINT Production on U.S. [Redacted] Field Exercises	A Signals Intelligence Directorate Management Directive that provides guidance to U.S. SIGINT System elements for issues related to SIGINT production on certain field exercises. The withheld information includes details of classified NSA activities, including communications intelligence (COMINT) sources and methods.	RIP	1 - classified information; 3 - 50 USC 3024(i), 18 USC 798, 50 USC 3605	10	22 Sep 14
7	10 Nov 10	OGC Legal Memorandum (Information Memorandum; AGC(IL)-756-2010)	A legal memorandum written by a senior NSA intelligence law attorney for the Deputy General Counsel analyzing a classified NSA SIGINT activity under EO 12333 and USSID 18. The analysis includes non-segregable details of classified NSA activities, including COMINT sources and methods.	DIF	1 - classified information; 3 - 50 USC 403, 18 USC 798, 50 USC 3605 5 - privilege	6	22 Sep 14

UNCLASSIFIED



UNCLASSIFIED

Documents Challenged by ACLU							
Doc No.	Doc. Date	Title	Description	Disposition	Exemption(s)	Pages	Production Date
9	22 Jan 08	OGC Legal Background Paper [TITLE CLASSIFIED]	A background paper on NSA authority under EO 12333 written by a senior NSA intelligence law attorney regarding a particular SIGINT activity. The paper includes non-segregable details of classified NSA activities, including COMINT sources and methods.	DIF	1 - classified information; 3 - 50 USC 403, 18 USC 798, 50 USC 3605	2	22 Sep 14
11	13 Jan 12	Legal Memorandum and Associated Approval Documentation [TITLE CLASSIFIED]	A legal memorandum written by DOJ concerning classified SIGINT activities undertaken pursuant to EO12333 and supporting documentation providing non-segregable details of classified NSA COMINT activities, sources, and methods.	DIF	1 - classified information; 3 - 50 USC 403, 18 USC 798, 50 USC 3605 5 - privilege	45	22 Sep 14
12	09 Jan 12	Approval Package for an NSA Program [TITLE CLASSIFIED]	Approval package for a classified NSA program, including a formal legal memorandum written by DOJ concerning classified COMINT activities undertaken pursuant to EO12333 and supporting documentation providing non-segregable details of classified NSA COMINT activities, sources, and methods.	DIF	1 - classified information; 3 - 50 USC 403, 18 USC 798, 50 USC 3605 5 - privilege	87	22 Sep 14
13	13 Jan 12	Memo Approving NSA Program [TITLE CLASSIFIED]	Documentation of approval for a classified NSA program undertaken pursuant to EO12333. The memo includes non-segregable details of classified NSA activities, including COMINT sources and methods.	DIF	1 - classified information; 3 - 50 USC 3024(i), 18 USC 798, 50 USC 3605	1	22 Sep 14

UNCLASSIFIED

UNCLASSIFIED

Documents Challenged by ACLU							
Doc No.	Doc. Date	Title	Description	Disposition	Exemption(s)	Pages	Production Date
14	14 Jun 13	OGC Legal Memorandum [TITLE CLASSIFIED]	A legal memorandum written by a senior NSA intelligence law attorney concerning classified SIGINT activities. The analysis includes non-segregable details of classified NSA activities, including COMINT sources and methods.	DIF	1 - classified information; 3 - 50 USC 403, 18 USC 798, 50 USC 3605 5 - privilege	5	22 Sep 14
15	16 May 12	OGC Legal Memorandum to SID Director [TITLE CLASSIFIED]	A legal memorandum written by a senior NSA intelligence law attorney for the Director of NSA's Signals Intelligence Directorate. The analysis includes non-segregable details of classified NSA activities, including COMINT sources and methods.	DIF	1 - classified information; 3 - 50 USC 403, 18 USC 798, 50 USC 3605 5 - privilege	1	22 Sep 14
16	04 Feb 11	OGC Legal Memorandum [TITLE CLASSIFIED]	A legal memorandum written by a senior NSA intelligence law attorney providing legal guidance to the Signals Intelligence Directorate on classified activities undertaken pursuant to EO12333 in support of NSA's SIGINT mission. The analysis includes non-segregable details of classified NSA activities, including COMINT sources and methods.	DIF	1 - classified information; 3 - 50 USC 3024(i), 18 USC 798, 50 USC 3605 5 - privilege	3	22 Sep 14
17	13 Feb 13	OGC Legal Memorandum, AGC(IL): 2013-4626 [TITLE CLASSIFIED]	A legal memorandum written by a senior NSA intelligence law attorney for the Director of NSA's Signals Intelligence Directorate regarding audits of SIGINT activities undertaken pursuant to EO12333. The analysis includes non-segregable details of classified NSA activities, including COMINT sources and methods.	DIF	1 - classified information; 3 - 50 USC 403, 18 USC 798, 50 USC 3605 5 - privilege	6	22 Sep 14

UNCLASSIFIED

UNCLASSIFIED

Documents Challenged by ACLU							
Doc No.	Doc. Date	Title	Description	Disposition	Exemption(s)	Pages	Production Date
18	14 Feb 13	OGC Legal Memorandum, AGC(IL): 2013-4640 [TITLE CLASSIFIED]	A legal memorandum written by a senior NSA intelligence law attorney for NSA senior leaders regarding the protection of US Person information under EO12333 and related regulations. The analysis includes non-segregable details of classified NSA activities, including COMINT sources and methods.	DIF	1 - classified information; 3 - 50 USC 403, 18 USC 798, 50 USC 3605 5 - privilege	7	22 Sep 14
19	28 Sep 11	OGC Legal Memorandum, Serial: GC/051/11 [TITLE CLASSIFIED]	A legal memorandum written by a senior NSA intelligence law attorney for the Signals Intelligence Directorate regarding the protection of US Person information during classified SIGINT activities undertaken pursuant to EO12333. The analysis includes non-segregable details of classified NSA activities, including COMINT sources and methods.	DIF	1 - classified information; 3 - 50 USC 403, 18 USC 798, 50 USC 3605 5 - privilege	4	22 Sep 14
20	25 May 12	OGC Legal Memorandum, AGC(IL): 2012-2912 [TITLE CLASSIFIED]	A legal memorandum written by a senior NSA intelligence law attorney for the Signals Intelligence Directorate regarding querying data collected pursuant to EO12333. The analysis includes non-segregable details of classified NSA SIGINT activities, including COMINT sources and methods.	DIF	1 - classified information; 3 - 50 USC 3024(i), 18 USC 798, 50 USC 3605 5 - privilege	8	22 Sep 14

UNCLASSIFIED

UNCLASSIFIED

Documents Challenged by ACLU							
Doc No.	Doc. Date	Title	Description	Disposition	Exemption(s)	Pages	Production Date
21	11 Feb 11	OGC Legal Memorandum [TITLE CLASSIFIED]	A legal memorandum written by a senior NSA intelligence law attorney for the Signals Intelligence Directorate regarding NSA's authority to conduct certain classified SIGINT activities. The analysis includes non-segregable details of classified NSA SIGINT activities, including COMINT sources and methods.	DIF	1 - classified information; 3 - 50 USC 403, 18 USC 798, 50 USC 3605 5 - privilege	5	22 Sep 14
22	01 Dec 07	IG Report on an NSA Program; IG-10853-07 [TITLE CLASSIFIED]	A report by the NSA Office of Inspector General on the intelligence oversight process connected to a classified NSA program. The report details classified NSA activities, including COMINT sources and methods.	DIF	1 - classified information; 3 - 50 USC 3024(i), 18 USC 798, 50 USC 3605	40	22 Sep 14
23	20 Sep 10	IG Report ST-09-0019 [TITLE CLASSIFIED]	A report by the NSA Office of Inspector General on classified NSA SIGINT activities. The report details such activities, including COMINT sources and methods.	DIF	1 - classified information; 3 - 50 USC 3024(i), 18 USC 798, 50 USC 3605	84	22 Sep 14
28	12 Jul 07	OGC Memorandum for the Deputy Chief of Staff, Subject: Sharing of "RAW SIGINT" Through Database Access	A legal memorandum from the NSA Associate General Counsel for Operations to the NSA Deputy Chief of Staff regarding the sharing of raw SIGINT through database access. The withheld information includes privileged legal analysis and details regarding NSA's organization, functions, and activities, including classified COMINT sources and methods.	RIP	1 - classified information; 3 - 50 USC 3024 (i), 18 USC 798, 50 USC 3605 5 - privilege	8	22 Oct 14

UNCLASSIFIED

UNCLASSIFIED

Documents Challenged by ACLU							
Doc No.	Doc. Date	Title	Description	Disposition	Exemption(s)	Pages	Production Date
79	4 March 2013	Quarterly Report to the President's Intelligence Oversight Board, 1 st Quarter FY2013.	One of 47 quarterly reports to the Intelligence Oversight Board (4Q 2001-2Q 2013) and 4 annual reports to the Intelligence Oversight Board (2007, 2008, 2009, 2010). The reports detail compliance issues reported to the IOB by the NSA Office of Inspector General and the Office of General Counsel.	RIP	1 - classified information; 3 - 50 USC 3024(i), 18 USC 798, 50 USC 3605	21	22 Dec 14
N/A (Bates No. 4086222)	25 January 2011	USSID SP0018: Legal Compliance and U.S. Persons Minimization Procedures	U.S. Signals Intelligence Directive that prescribes policies and procedures and assigns responsibilities to ensure that the missions and functions of the United States SIGINT system are conducted in a manner that safeguards the constitutional rights of U.S. persons.	RIP	1 - classified information; 3 - 50 USC 3024(i), 18 USC 798, 50 USC 3605	52	18 Nov 13
N/A (Bates No. 4086223)	24 April 1986	USSID SP0018J: Procedures for Monitoring Radio Communications of Suspected International Narcotics Traffickers	An Annex to USSID SP0018 that regulates certain SIGINT activities against the radio communications of suspected international narcotics traffickers.	RIP	1 - classified information; 3 - 50 USC 3024(i), 18 USC 798, 50 USC 3605	8	18 Nov 13

UNCLASSIFIED

DOCID: 4275162

~~SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108~~

OFFICE OF GENERAL COUNSEL

MEMORANDUM FOR THE DEPUTY CHIEF OF STAFF

THRU: GC

SUBJECT: (U) SHARING OF "RAW SIGINT" THROUGH DATABASE ACCESS

(U//~~FOUO~~) You have asked us to conduct a legal review in order to set out the limits -- and the rationale associated with the limits -- on allowing personnel from other agencies access to NSA databases under the existing rules governing such access, and the advisability of changes to the Executive Order that would allow other agencies access to SIGINT databases.

(U//~~FOUO~~) We conclude that compliance with NSA's Attorney General-approved minimization procedures, which are required by Executive Order 12333 and are rooted in Fourth Amendment privacy protections, constrains NSA from granting to employees of other intelligence agencies widespread access to NSA content databases. These same procedures, largely for the same reasons, preclude such access for employees of customer agencies as well. By contrast, broad access to databases that contain exclusively communications metadata may lawfully be provided to other intelligence agencies, because communicants do not enjoy a constitutional expectation of privacy in such information. As a consequence, the Executive Order contemplates its widespread sharing among intelligence agencies.

(U//~~FOUO~~) [Redacted] (b)(3)-P.L. 86-36 (5)

[Large redacted area]

I. (U) SIGINT Dissemination Authorities and Limitations

(U//~~FOUO~~) NSA's authority to collect, retain, and disseminate SIGINT is both established and limited by Executive Order 12333, United States Intelligence Activities, and promulgated in various departmental and agency policies.¹ In general, the Executive Order

¹ (U) E.O. 12333 assigns NSA the responsibility for dissemination of SIGINT information. The first Executive Order establishing the intelligence community and authorizing entities within it to conduct particular intelligence activities was an outgrowth of the investigations in the 1970s by committees chaired by Senator Church and Representative Pike. These committees uncovered various abuses by intelligence agencies that concerned the collection, retention and dissemination of information concerning U.S. persons, leading to both the Executive Order

Derived From: NSA/CSSM 1-52

Dated: 20070108

Declassify On:

~~SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108~~

Approved for Release by NSA on 10-21-2014 FOIA Case #1

EXHIBIT
tabbles
AEX 14

DOCID: 4275162

~~SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108~~
ATTORNEY CLIENT PRIVILEGE: NO RELEASE OUTSIDE NSA WITHOUT OGC APPROVAL

requires that all intelligence agencies – including NSA -- comply with Attorney General-approved procedures before disseminating information concerning U.S. persons to other entities. Such procedures, the aim of which is to protect the privacy of U.S. persons, require each agency to make conscious determinations about the information it seeks to disseminate.

(U//~~FOUO~~) At the same time, the Executive Order makes a broad exception to this general rule with respect to dissemination of information within the Intelligence Community (IC). Specifically, it authorizes each agency within the IC – notwithstanding other procedural requirements -- to disseminate information to other appropriate agencies within the IC “for the purposes of allowing the recipient agency to determine whether the information is relevant to its responsibilities and can be retained by it.”

(U//~~FOUO~~) This broad authority to disseminate information to other agencies in the intelligence community without first applying minimization procedures -- itself an exception to the more general restriction on disseminating information concerning U.S. persons -- does not apply to “information derived from signals intelligence.”² This is so because of the underlying constitutional concerns associated with the acquisition of SIGINT by the government. Specifically, the Supreme Court held 40 years ago that when the government engages in electronic surveillance, it is conducting a search and seizure under the Fourth Amendment; therefore the activity must be carried out in a manner that is reasonable, the touchstone requirement of the Fourth Amendment.

~~(S//SI)~~ [Redacted]

[Redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(5)

~~(S//SI)~~ The Courts and Congress have long recognized, in light of the Fourth Amendment, that the appropriate manner in which to address the overbreadth that inheres in the act of conducting electronic surveillance is through the careful application of “minimization and to the Foreign Intelligence Surveillance Act (FISA), as well as oversight from Congressional committees.

² (U//~~FOUO~~) EO 12333, Part 2.3, Collection of Information, states:

Agencies within the Intelligence Community are authorized to collect, retain or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, consistent with the authorities provided by Part 1 of this Order. In addition, agencies within the Intelligence Community may disseminate information, other than information derived from signals intelligence, to each appropriate agency within the Intelligence Community for purposes of allowing the recipient agency to determine whether the information is relevant to its responsibilities and can be retained by it. [Redacted]

[Redacted]

(b)(3)-P.L. 86-36
(b)(5)

DOCID: 4275162

~~SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108~~
ATTORNEY CLIENT PRIVILEGE: NO RELEASE OUTSIDE NSA WITHOUT OGC APPROVAL

procedures,” procedures designed to reasonably limit the presence of non-pertinent information at each stage of the activity – collection, retention and dissemination. The Attorney General-approved procedures required for every intelligence agency by the Executive Order serve the policy goal of preventing the circulation of information concerning U.S. persons around the government without good reason. The procedures take on additional significance based on constitutional concerns in the case of SIGINT. Compliance with these procedural requirements is what rescues SIGINT activities from potentially plausible charges of unconstitutionality:

[Redacted] (b)(5) (b)(3)-P.L. 86-36

~~(S//SI)~~ Constitutionally protected SIGINT information cannot be disseminated, even within the IC, unless NSA first subjects such information to the minimization procedures required by Executive Order 12333. Among the requirements of these procedures are: (1) dissemination of signals intelligence shall be limited to authorized signals intelligence consumers in accordance with requirements and tasking established pursuant to Executive Order 12333, and (2) information that identifies a U.S. person may be disseminated only if one of a group of criteria can be satisfied; these criteria can be generally summarized as a requirement that NSA determine that the identifying information is necessary to understand the foreign intelligence or assess its significance. For the same reasons, entities outside the IC cannot, consistent with the Attorney General-approved minimization procedures, be provided access to databases containing unprocessed and unminimized SIGINT information.

2. (U//~~FOUO~~) Sharing Metadata vs. Sharing Content

~~(S//SI)~~ While the above reflects the current treatment of SIGINT information under the Executive Order and NSA’s Attorney General-approved procedures, a significant bright line distinction has evolved in the years since these were drafted. Specifically, NSA employs analysis of what it calls communications “metadata” – information that helps to effectuate communications but is not part of the substantive communication itself -- both as an end in itself and to guide and inform its collection of SIGINT content. While metadata is information derived from SIGINT, and thus is formally subject to the same procedural requirements prior to dissemination as is content, the underlying constitutional concerns that distinguish SIGINT from other intelligence activities do not exist in the metadata context. Indeed, the Supreme Court held in 1979 that a person does not enjoy a constitutional expectation of privacy in the numbers he dials on his telephone, even while he does enjoy such an expectation in the conversation that follows.⁴ While statutory protection still exists with respect to communications metadata, we

~~(TS//SI)~~ [Redacted] (b)(5) 86-36

⁴~~(S//SI)~~ The Department of Justice has adopted the position that this analysis extends to other signaling, dialing, routing and addressing information other than the numbers one dials on his telephone, and NSA OGC concurs.

[Redacted]

DOCID: 4275162

~~SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108~~
ATTORNEY CLIENT PRIVILEGE: NO RELEASE OUTSIDE NSA WITHOUT OGC APPROVAL

have concluded that greater flexibility exists as a matter of law with respect to the dissemination of communications metadata than exists with respect to dissemination of content.

(b) (1)
(b) (3)-P.L. 86-36

~~(S//SI)~~ Acting on the distinction between content and metadata and the legal consequences that flow therefrom [redacted] NSA has contributed bulk telephony metadata, after masking the numbers that contain U.S. area codes,⁵ to the interagency [redacted] database, where analysts from other intelligence agencies can and do access and analyze it.⁶

(b) (3)-P.L. 86-36

~~(S//SI)~~ In concurring with the dissemination of communications metadata to other IC agencies, OGC relied on two related notions. First, access to this body of metadata as a whole after automatically masking U.S. telephone numbers is consistent with the provision of the Executive Order authorizing each agency to provide acquired information to other appropriate agencies within the IC. [redacted]

(b)(3)-P.L. 86-36

[Large redacted block]

~~(S//SI)~~ For the reasons set out above, OGC believes that sharing of SIGINT metadata with any U.S. person identifying information removed is permissible currently, with no change to any authorities, and such dissemination is taking place with respect to telephony metadata, and prospects are good for much more robust sharing within the IC in the near future.⁷

0225P (6th Cir. June 18, 2007) at 32 (third party subpoena to service provider to access information that is shared with it *likely* creates no Fourth Amendment problem) (emphasis added).

⁵ (U//FOUO) The legislative history of the FISA makes clear that Congress believed a U.S. telephone number is information that identified a U.S. person.

⁶ ~~(S//SI)~~ NSA masks the U.S. telephone numbers for two reasons, one more important than the other: first, NSA does so because it is constrained by its AG-approved procedures to disseminate information that identifies U.S. persons only when it has first concluded that the information is necessary to understand or assess the significance of foreign intelligence. Second, and more significantly, every intelligence agency is prohibited by Executive Order from asking another to do what it cannot lawfully do itself. [redacted]

[redacted]

[redacted]

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)
(b) (5)

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)

DOCID: 4275162

~~SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108~~
ATTORNEY CLIENT PRIVILEGE: NO RELEASE OUTSIDE NSA WITHOUT OGC APPROVAL
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

~~(S//SI)~~ As a practical matter, metadata from electronic communications such as e-mail cannot be similarly shared at the moment under the same theory, because it is not possible to determine what communications are to or from U.S. persons nearly as readily as is the case with telephony, and often is not possible at all. [Redacted]

[Redacted]

3. (U//~~FOUO~~) Potential Changes to E.O. 12333 & AG-approved Dissemination Procedures

(U//~~FOUO~~) Finally, as part of the DNI information sharing initiative, the DNI received Presidential approval to recommend revisions to Executive Order 12333. The ODNI OGC is reviewing the document and will provide recommendations to the DNI by October 2007; the NSA OGC is the NSA lead on this action, and is in contact with the ODNI concerning it.

(b)(3)-P.L. 86-36
(b)(5)

(U//~~FOUO~~) [Redacted]

~~(S//SI)~~ [Redacted]

[Redacted]

~~(S//SI)~~ [Redacted]

(b)(3)-P.L. 86-36
(b)(5)

(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)
(b)(5)

DOCID: 4275162

~~SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108~~
ATTORNEY CLIENT PRIVILEGE: NO RELEASE OUTSIDE NSA WITHOUT OGC APPROVAL

[Redacted]

(b)(3)-P.L. 86-36
(b)(5)

(S//SI)

[Redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(5)

- [Redacted]

- [Redacted]

- [Redacted]

- [Redacted]

- [Redacted]

* (U//FOUO) In addition to the language of Section 2.3, the Executive Order also states that no Department or agency other than NSA may engage in signals intelligence activities except pursuant to a delegation by the Secretary of Defense. Section 1.11(b). This provision might also have to be changed in order to effect database access for other agencies.

DOCID: 4275162

~~SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108~~
ATTORNEY CLIENT PRIVILEGE: NO RELEASE OUTSIDE NSA WITHOUT OGC APPROVAL

• [Redacted] (b)(1)
(b)(3)-P.L. 86-36
(b)(5)

• [Redacted]

[Redacted] (b)(5)
(b)(3)-P.L. 86-36

~~(S//SI)~~ [Redacted] (b)(3)-P.L. 86-36
(b)(5)

4. (U//~~FOUO~~) Conclusion

~~(S//SI)~~ There are substantial and well-grounded legal limits on NSA's ability to provide its partners and customers with access to raw SIGINT databases, both those that contain content and those that contain only metadata. Within those limits, NSA has lawfully expanded that access in two ways: with respect to content, we have expanded access by bringing IC partners within the SIGINT production chain in carefully defined circumstances. With respect to metadata, we have aggressively pushed telephony metadata to IC partners, and have plans in place to increase dramatically both the types and the completeness of the metadata we share.

~~(S//SI)~~ Based on the legal and prudential considerations set out above, it seems that access to metadata can and should be widespread within the IC, including military intelligence units, and should be used as a tool to inform and adjust content collection requirements. In the absence of concrete benefit to the intelligence community in meeting the needs of the nation, we think that further requests for broader access to unevaluated and unminimized SIGINT content databases should continue to be on a case-by-case basis, rather than a wholesale basis, and should be the exception rather than the rule. Further, any decision to initiate a change to the NSA's procedures should be considered in light of the benefits weighed against what we think are genuine and serious risks.

(U//~~FOUO~~) Please contact us if you would like to discuss this issue further.

//s//

[Redacted]
Associate General Counsel
(Operations)

(b) (3) - P.L. 86

July 12, 2007

DOCID: 4275162

~~SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108~~
ATTORNEY CLIENT PRIVILEGE: NO RELEASE OUTSIDE NSA WITHOUT OGC APPROVAL

~~SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL//20320108~~

DOCID: 4165220

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~



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

4 March 2013

MEMORANDUM FOR THE CHAIRMAN, INTELLIGENCE OVERSIGHT BOARD

THRU: Assistant to the Secretary of Defense (Intelligence Oversight)

SUBJECT: (U//~~FOUO~~) Report to the Intelligence Oversight Board on NSA Activities -
INFORMATION MEMORANDUM

(U//~~FOUO~~) Except as previously reported to you or the President, or otherwise stated in the enclosure, we have no reason to believe that intelligence activities of the National Security Agency during the quarter ending 31 December 2012 were unlawful or contrary to Executive Order or Presidential Directive and thus should have been reported pursuant to Section 1.6(c) of Executive Order 12333, as amended.

(U//~~FOUO~~) The Inspector General and the General Counsel continue to exercise oversight of Agency activities by inspections, surveys, training, review of directives and guidelines, and advice and counsel.

George Ellard
GEORGE ELLARD
Inspector General

Rajesh De
RAJESH DE
General Counsel

(U//~~FOUO~~) I concur in the report of the Inspector General and the General Counsel and hereby make it our combined report.

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

Encl:
Quarterly Report

This document may be declassified and marked
"UNCLASSIFIED//~~For Official Use Only~~"
upon removal of enclosure(s)

Approved for Release by NSA on 12-19-2014, FOIA Case # 70809 (Litigation)

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~



DOCID: 4165220

REF ID:A4131753

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

I. (U) Intelligence, Counterintelligence, and Intelligence-Related Activities that Violated Law, Regulation, or Policy and Were Substantiated during the Quarter, as well as Actions Taken as a Result of the Violations

I.A. (U) Intelligence Activities Conducted under Executive Order (E.O.) 12333 Authority

(U//~~FOUO~~) Some incidents may involve more than one authority (e.g., E.O. 12333, NSA/CSS Title I Foreign Intelligence Surveillance Act (FISA), FISA Amendments Act (FAA). Incidents involving more than one authority are included in the section for each involved authority. Thus, a single incident may produce multiple entries in this report.

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 3024 (i)

I.A.1 (U) Unintentional Targeting or Database Queries against United States Persons (USPs) or Foreign Persons in the United States

~~(S//SI//REL TO USA, FVEY)~~ During the fourth quarter of calendar year 2012 (CY2012), the National Security Agency/Central Security Service (NSA/CSS) continued [redacted] [redacted] As part of that process, duplicate selectors were removed and the number of active selectors was reduced. At the end of the fourth quarter of CY2012, NSA/CSS's primary tasking tools for telephone and Internet selectors contained approximately [redacted] active selectors.

(b) (3)-P.L. 86-36

(U//~~FOUO~~) During the fourth quarter of CY2012, in [redacted] instances, signals intelligence (SIGINT) analysts inadvertently targeted communications to, from, or about USPs, while pursuing foreign intelligence tasking or performed mistaken queries that potentially sought or returned information about USPs. Unless otherwise specified, all intercepts, query results, and reports have been deleted or destroyed as required by United States SIGINT Directive SP0018.

I.A.1.a. (U) Tasking Errors

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an analyst discovered that selectors associated with a USP had erroneously been tasked because the analyst had overlooked information about the target's USP status. All selectors associated with the target were detasked, and all collected data was purged.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an analyst discovered that a selector for a foreign intelligence target that had been detasked was subsequently retasked while the target was in the United States. The analyst detasked the selector [redacted]

(b) (1)
(b) (3)-P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~ [redacted] analysts discovered that selectors associated with foreign intelligence targets that had been previously detasked because [redacted] were retasked while the targets were in the United States. All selectors were detasked and no collection occurred.

~~(TS//SI//NF)~~ [redacted] an analyst discovered that [redacted] selectors associated with a USP had been erroneously tasked because information about the target's USP status was

Derived From: NSA/CSSM 1-52, dated 20080107

Declassify On: 20380304

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

(b)(1)
(b)(3)-P.L. 86-36

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 3024(i)

not provided by an Intelligence Community (IC) customer when the selector was being researched for tasking. The selector was detasked, and all data was deleted [redacted]

~~(TS//SI//TK//REL TO USA, FVEY)~~ [redacted]

[redacted] were erroneously targeted and collection occurred for 39 minutes because a [redacted] before executing the collection task. All collected data was purged.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an analyst mistakenly requested tasking of his own personal identifier instead of the selector associated with a foreign intelligence target. The selector was detasked [redacted]

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 3024(i)

I.A.1.a.i. (U) **Unauthorized Targeting**

~~(TS//SI//NF)~~ [redacted] an analyst discovered that a telephone selector associated with a USP, formerly approved for targeting under a [redacted]

[redacted] was tasked [redacted] The selector was detasked [redacted]

[redacted] A destruction waiver has been requested, and a request for FAA §704 authorization has been submitted for future targeting.

(b) (1)
(b) (3)-P.L. 86-36

~~(TS//SI//NF)~~ [redacted] an analyst discovered that data had been collected [redacted] on the selector for a foreign intelligence target when the target was in the United States. [redacted]

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 3024(i)

I.A.1.b. (U) **Database Queries**

~~(S//SI//REL TO USA, FVEY)~~ [redacted]

[redacted]

(U//~~FOUO~~) On [redacted] occasions during the fourth quarter, analysts performed overly broad or poorly constructed database queries that potentially selected or returned information about USPs. These queries used [redacted]

[redacted] that produced imprecise results. On [redacted] of those occasions, the queries returned results, which were deleted or aged off, as required, and no reports were issued. Analysts who performed these queries were counseled by their management.

(U) Procedural and other errors contributed to the following incidents: (b) (3)-P.L. 86-36

- ~~(S//SI//REL TO USA, FVEY)~~ On [redacted] occasions during the fourth quarter, NSA analysts performed queries in raw traffic databases without first conducting the necessary research

(b) (1)
(b) (3)-P.L. 86-36

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

on the selectors. When the queries returned results, they were deleted and no reports were issued.

- ~~(TS//SI//REL TO USA, FVEY)~~ While performing a query on a selector for a foreign intelligence target [redacted] [redacted] NSA had detasked the selector because the target was in the United States. The query results were deleted. [redacted] (b) (1) (b) (3) - P.L. 86-36
- ~~(S//SI//REL TO USA, FVEY)~~ [redacted] an analyst performed a query in a raw traffic database [redacted] (b) (1) (b) (3) - P.L. 86-36 (b) (3) - 50 USC 3024(i)
- ~~(S//REL TO USA, FVEY)~~ [redacted]
- ~~(S//SI//REL TO USA, FVEY)~~ [redacted] a database auditor discovered that an analyst had mistakenly performed [redacted] queries in a raw traffic database on the selectors for a foreign intelligence target in the United States. The analyst deleted the results. (b) (1) (b) (3) - P.L. 86-36
- ~~(S//SI//REL TO USA, FVEY)~~ [redacted] an analyst performed a query in a raw traffic database on a selector that had been determined [redacted] to be associated with a USP. The analyst deleted the query and results [redacted]
- ~~(S//SI//REL TO USA, FVEY)~~ [redacted] in a raw traffic database on selectors associated with a target when it was known that [redacted] the United States [redacted]
- ~~(S//SI//REL TO USA, FVEY)~~ [redacted] an analyst performed a query using a selector associated with a USP [redacted] The analyst then sent the results of the query to another analyst. Subsequently, the analyst learned that the selector was registered to a USP. The analyst recalled the e-mail and deleted all query results.
- ~~(TS//SI//NF)~~ [redacted] analysts selected an incorrect database when performing queries on selectors associated with foreign intelligence targets. No results were returned. (b) (1) (b) (3) - P.L. 86-36
- ~~(TS//SI//NF)~~ [redacted] a database auditor discovered that an analyst had mistakenly performed a query on a target authorized under FAA §705(b) [redacted] [redacted] a raw traffic database during the time the target was in the United States. The query and results were deleted [redacted]

(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 50 USC 3024(i)

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

- ~~(S//SI//REL TO USA, FVEY)~~ [redacted] an analyst discovered that a query was performed on a selector associated with a foreign intelligence target while the target was in the United States.

- ~~(TS//SI//REL TO USA, FVEY)~~ [redacted] in a raw traffic database on one of the selectors for a foreign intelligence target who arrived in the United States [redacted]. The analyst was [redacted] because of database access problems. The results were deleted [redacted].

(b) (1)
(b) (3)-P.L. 86-36

- ~~(S//SI//REL TO USA, FVEY)~~ [redacted] an analyst performed a query in the incorrect raw SIGINT database. The query and the results were deleted immediately.

- ~~(S//SI//REL TO USA, FVEY)~~ [redacted] an analyst unfamiliar with a query tool performed a query in a raw traffic database [redacted]. No results were returned.

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 3024 (i)

- ~~(TS//SI//REL TO USA, FVEY)~~ On three occasions [redacted] analysts discovered [redacted] the selectors associated with foreign intelligence targets were detasked because [redacted] the United States [redacted] results were deleted.

(b) (1)
(b) (3)-P.L. 86-36

- ~~(S//SI//REL TO USA, FVEY)~~ [redacted] an analyst performed a query in a raw traffic database on a list of selectors that included one associated with a USP. Upon discovery of the error, the analyst stopped the query and removed the selector.

- ~~(S//SI//REL TO USA, FVEY)~~ [redacted] an analyst included a U.S. e-mail address instead of the intended target's e-mail address in a query running in a raw traffic database. No results were returned.

- ~~(S//SI//REL TO USA, FVEY)~~ [redacted] an analyst performed a query in a raw traffic database [redacted]. The analyst deleted the results without viewing them [redacted].

- ~~(TS//SI//NF)~~ [redacted] an analyst performed a query in a raw traffic database on a selector associated with a USP. A destruction waiver was approved [redacted].

- ~~(S//SI//REL TO USA, FVEY)~~ [redacted] an analyst ran a query in a raw traffic database on the selectors associated with a foreign intelligence target while the target was in the United States. The analyst deleted the query and results [redacted].

- ~~(S//SI//REL TO USA, FVEY)~~ [redacted] an analyst performed a query in a raw traffic database on the incorrect selector because [redacted] into the query form. The query was canceled before execution, and no results were returned.

(b) (1)
(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 3024 (i)

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)

I.A.1.c. (U) **Detasking Delays**

~~(S//SI//REL TO USA, FVEY)~~ A selector associated with a foreign intelligence target

[redacted]
[redacted] The delay occurred because [redacted]
[redacted] No collection
occurred.

~~(S//SI//REL TO USA, FVEY)~~ [redacted] it was discovered that selectors for [redacted] foreign intelligence targets had been overlooked for detasking and remained on task. Upon discovery, the selectors were detasked.

~~(S//SI//REL TO USA, FVEY)~~ [redacted] during a selector review, an analyst noticed that a selector for a foreign intelligence target that had been detasked [redacted] [redacted] The selector was detasked.

(b) (1)
(b) (3)-P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~ [redacted] when retasking a selector for a foreign intelligence target, an analyst discovered that the selector had remained on task while the target was in the United States. No collection occurred during the time the target was in the United States.

~~(S//SI//REL TO USA, FVEY)~~ [redacted] it was discovered that selectors for a foreign intelligence target had remained on task despite information [redacted] [redacted] the United States. All selectors were detasked [redacted]

~~(S//SI//REL TO USA, FVEY)~~ [redacted] an analyst learned that a selector for a foreign intelligence target had been overlooked when [redacted]

[redacted]
[redacted] The selector was detasked [redacted]

~~(TS//SI//REL TO USA, FVEY)~~ Selectors for a foreign intelligence target remained on task [redacted] after NSA analysts had detasked the selectors because the target had entered the United States [redacted] No reports were issued.

(b) (1)
(b) (3)-P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~ [redacted] analysts learned that selectors for a foreign intelligence target [redacted] the United States [redacted] had remained on task despite the submission of a detask request [redacted] The selectors were detasked [redacted] and data was purged.

(b) (1)
(b) (3)-P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~ [redacted] an analyst discovered that selectors remained on task for a foreign intelligence target [redacted] the United States [redacted]

[redacted]
[redacted]
[redacted] The selectors were detasked [redacted]

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] it was discovered that [redacted] selectors for a foreign intelligence target had been overlooked when other selectors tasked under FAA §702 authority were detasked because of the target's U.S. travel. All selectors were detasked, and non-compliant FAA §702 data has been marked for purging. It was also discovered that the selectors [redacted] in a raw traffic database. [redacted] and the selectors were removed [redacted]

(b) (1)
(b) (3) - P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~ [redacted] delays in detasking the selectors for a foreign intelligence target who had entered the United States [redacted] [redacted] The selectors were detasked and no data was collected.

~~(S//SI//REL TO USA, FVEY)~~ [redacted] an analyst learned that a selector for a foreign intelligence target had remained on task even though information was known on [redacted] about the target's U.S. travel. The selector was detasked [redacted] No collection occurred.

~~(S//SI//REL TO USA, FVEY)~~ [redacted] selectors for foreign intelligence targets were discovered to have remained on task, even though related selectors had been detasked because the targets were in the United States. Upon discovery, the selectors were detasked.

(b) (1)
(b) (3) - P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~ [redacted] an analyst discovered that [redacted] valid foreign intelligence targets had traveled to the United States from [redacted] Although information was available [redacted] in the forwarding of the information. Upon discovery of the information [redacted] the analyst initiated the detasking. Collection was deleted, and no reporting occurred.

(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 18 USC 798
(b) (3) - 50 USC 3024 (i)

I.A.2 (U) [redacted]

~~(S//SI//REL TO USA, FVEY)~~ [redacted]
[redacted]

I.A.3 (U) Unauthorized Access

(b) (1)
(b) (3) - P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~ [redacted] it was discovered at NSA/CSS Colorado (NSAC) that approximately [redacted] personnel, not all of whom had the proper authority or training, had had access to the [redacted]

[redacted]

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 50 USC 3024 (i)

[Redacted]

[Redacted] NSAC has begun an in-depth review of all raw SIGINT data sources to ensure that raw SIGINT is being handled properly.

(b) (3)-P.L. 86-36

(U//FOUO) [Redacted] it was discovered that raw SIGINT data was stored on a server not authorized to hold it. The data was deleted and moved to an authorized location. A listing of authorized servers has been compiled to prevent future errors.

I.A.4 (U) Data-Handling Error

~~(TS//SI//REL TO USA, FVEY)~~ [Redacted] an analyst forwarded an e-mail to unauthorized recipients that included the identities of USPs. The e-mail was immediately recalled.

(b) (1)
(b) (3)-P.L. 86-36

~~(S//SI//NF)~~ [Redacted] an analyst forwarded in an e-mail to unauthorized recipients the results of a raw traffic database query that included terms associated with a USP. The e-mail was recalled the same day.

~~(C//SI//NF)~~ [Redacted] NSA issued a memorandum that erroneously contained a USP identity. The memorandum was immediately recalled.

(b) (1)
(b) (3)-P.L. 86-36

~~(TS//SI//NF)~~ [Redacted] USP information was inadvertently released as part [Redacted] were not vetted for possible USP data. The recipient has submitted a request for evaluated minimized traffic.

~~(TS//SI//REL TO USA, FVEY)~~ [Redacted] USP information was released to unauthorized recipients in a chat room. The information was recalled, and the recipients were instructed to destroy all copies.

~~(TS//SI//REL TO USA, FVEY)~~ [Redacted] an NSA analyst provided a file containing raw SIGINT to an IC analyst who was not authorized to receive it. Upon discovery of his mistake [Redacted] the NSA analyst instructed the IC analyst to delete the file.

~~(TS//SI//REL TO USA, FVEY)~~ [Redacted] an analyst discovered that the identity of a U.S. entity had not been masked in traffic passed [Redacted]. The traffic was canceled, properly minimized, and reissued [Redacted]. [Redacted] purged the traffic containing the unmasked U.S. identity. To prevent a recurrence, [Redacted]

(b) (1)
(b) (3)-P.L. 86-36

I.A.5 (U) Systems Error

~~(TS//SI//NF)~~ [Redacted] it was discovered that a system [Redacted] without sufficient [Redacted]

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

documentation regarding the system's procedures for data ingest, age-off, or purge. Information gathered [redacted] indicated that the data retained in the system included

[redacted] Efforts to identify the scope of the problem, as well as solutions, are ongoing.

(b) (1)
(b) (3)-P.L. 86-36

I.B. (U) Foreign Intelligence Surveillance Act (FISA)

(U//~~FOUO~~) Some incidents may involve more than one authority (e.g., E.O. 12333, NSA/CSS Title I FISA, FAA). Incidents involving more than one authority are included in the section for each involved authority. Thus, a single incident may produce multiple entries in this report.

(U//~~FOUO~~) Incidents of non-compliance with any authority or approval granted by the Foreign Intelligence Surveillance Court (FISC) are reported to the FISC, the Department of Justice, and the Office of the Director of National Intelligence.

I.B.1. (U) NSA/CSS Title I FISA

I.B.1.a. (U) Detasking Delays

(~~TS//SI//NF~~) [redacted] analysts discovered that selectors for foreign intelligence targets had not been detasked [redacted]. All selectors have been detasked, and non-compliant data has been marked for purging.

(~~TS//SI//NF~~) [redacted] an analyst discovered that a selector associated with a previously FISC-approved target [redacted] had been mistakenly included on a renewal of the Court Order [redacted].

(b) (1)
(b) (3)-P.L. 86-36

I.B.1.b. (U) Unauthorized Targeting

(~~TS//SI//NF~~) [redacted] an analyst discovered that communications collected pursuant to FISA authority did not belong to the FISC-approved target. The selector used to target the communications was detasked and non-compliant data was marked for purging.

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

Data collected from the selector has been requested to be purged.

(~~TS//SI//NF~~) [redacted] an analyst learned that [redacted] had been using the telephone number for a [redacted]. The telephone selector was detasked, and non-compliant data was marked for purging.

(b) (1)
(b) (3)-P.L. 86-36

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

~~TOP SECRET//SI//ALENT KEYHOLE//NOFORN~~

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-18 USC 798

(TS//SI//NF) [redacted] an analyst discovered that a tasked telephone selector was associated with a U.S. entity. The data was purged [redacted]

(TS//SI//NF) [redacted] an analyst discovered that collection occurring on a cellular telephone selector associated with a FISC-approved target [redacted] The selector

(b) (1)
(b) (3)-P.L. 86-36

(TS//SI//NF) [redacted] it was discovered that a cellular telephone number authorized for collection under a FISC Order [redacted]

[redacted] The selector was detasked [redacted] and non-compliant data was requested to be purged [redacted]

I.B.1.c. (U) Database Queries

(TS//SI//NF) [redacted] an analyst performed a query in a raw traffic database on the selectors associated with a target after it had been determined that the target was no longer considered to be an agent of a foreign power. Non-compliant data was marked for purging.

I.B.1.d. (U) Data-Handling Errors

(b) (1)
(b) (3)-P.L. 86-36

(TS//SI//NF) [redacted] while investigating an incident of improper handling of [redacted] NSA discovered that analysts in various organizations were not handling Title I FISA data properly. NSA provided remedial training to analysts who access Title I FISA data.

(S//SI//REL TO USA, FVEY) [redacted] an analyst discovered that [redacted] reported to the compliance organization [redacted] The work to determine the scope of the problem and the steps to mitigate the incidents is ongoing.

I.B.2. (S//REL TO USA, FVEY) [redacted]

(U) Nothing to report.

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 3024(i)

I.B.3. (TS//SI//NF) Business Records (BR) Order

I.B.3.a. (U) Data-Handling Error

(TS//SI//NF) [redacted] it was discovered that metadata obtained under the FISA BR Court Order had been released in an e-mail [redacted] counterparts without required approval. The personnel involved were counseled on the proper dissemination procedures. Ultimately, the required approval was obtained, and, therefore, the e-mail was not recalled.

(b) (1)
(b) (3)-P.L. 86-36

~~TOP SECRET//SI//ALENT KEYHOLE//NOFORN~~

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

I.B.4. (U) FISA Amendments Act (FAA)

(U//~~FOUO~~) Some incidents may involve more than one authority (e.g. E.O. 12333, NSA/CSS Title I FISA, FAA). Incidents involving more than one authority are included in the section for each involved authority. Thus, a single incident may produce multiple entries in this report.

I.B.4.a. (U) FAA Section 702

(b) (3) - P.L. 86-36

(U//~~FOUO~~) NSA/CSS has implemented a process to ensure that FAA §702 data required to be purged is purged from NSA/CSS databases. NSA created a [redacted] [redacted] to identify non-compliant data that should be purged.

I.B.4.a.i. (U) Tasking Errors

(~~TS//SI//REL TO USA, FVEY~~) On [redacted] occasions during the fourth quarter, selectors were incorrectly tasked because of typographical errors. The selectors were detasked, and the information has been purged. No reports were issued.

(~~TS//SI//REL TO USA, FVEY~~) On [redacted] occasions, it was discovered that a selector had been tasked in error because the target did not meet the criteria of an FAA §702 certification. The selectors have been detasked, and the non-compliant data has been purged. No reports were issued.

(~~TS//SI//REL TO USA, FVEY~~) [redacted] it was discovered that a selector had been erroneously tasked because information received [redacted] about the target's USP status had not been passed to the analyst before the selector was approved for tasking. In addition, the selector had remained on task [redacted] because of confusion about which analyst would submit the detask request. All non-compliant data has been marked for purging, and no reports were issued.

(~~TS//SI//REL TO USA, FVEY~~) [redacted] an analyst discovered that a selector tasked under the FAA §702 [redacted] certification should have been tasked under the [redacted] certification. The selector was detasked [redacted] and all non-compliant data was marked for purging.

(b) (1)
(b) (3) - P.L. 86-36 (~~TS//SI//REL TO USA, FVEY~~) [redacted] it was discovered that a selector was erroneously tasked [redacted] Upon discovery, the selector was immediately detasked. The non-compliant data was marked for purging.

(~~TS//SI//NF~~) [redacted] it was discovered that a selector had been retasked in error because an analyst had not followed proper tasking procedures. The selector had been detasked [redacted] [redacted] The selector was detasked [redacted] Non-compliant data has been marked for purging.

(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 18 USC 798

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 50 USC 3024 (1)

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] it was discovered that a selector associated with a valid foreign intelligence target had been erroneously tasked because of a typographical error. Believed to be associated with a USP, the incorrect selector had been detasked, and non-compliant data has been marked for purging.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an analyst learned that a selector had been erroneously tasked because an IC agency analyst had passed an incorrect selector. The selector was detasked [redacted] and non-compliant data has been marked for purging.

(b) (1)
(b) (3) - P.L. 86-36

~~(TS//SI//NF)~~ [redacted] an analyst discovered [redacted] that a valid foreign intelligence target had been in communications with another person, while both were located in the United States. All non-compliant data associated with the domestic communication was purged, and no reports were issued.

(b) (3) - P.L. 86-36
(b) (3) - 50 USC 3024 (i)

~~(TS//SI//REL TO USA, FVEY)~~ On [redacted] occasions, an analyst tasked a selector believed to be associated with a valid foreign intelligence target, but after tasking, the analyst received proof that the target was either a USP or not the intended target. In each situation, the selector was detasked and the non-compliant data was purged.

I.B.4.a.ii. (U) Unauthorized Targeting

(b) (1)
(b) (3) - P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ On [redacted] occasions during the fourth quarter, collection occurred on e-mail accounts [redacted] the United States [redacted]

[redacted] (Also included are occasions when [redacted] the United States could not be confirmed.)

I.B.4.a.iii. (U) Database Queries

(b) (1)
(b) (3) - P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ On [redacted] occasions during the fourth quarter, analysts performed in FAA §702 data overly broad or poorly constructed database queries that potentially selected or returned information about USPs. These queries used [redacted]

[redacted] that produced imprecise results.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an analyst performed a query in an FAA §702 raw traffic database using selectors associated with a USP target approved under FAA §705(b) authority. The queries were not performed in accordance with NSA internal procedures. The query and the results were deleted.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an analyst learned that a selector associated with a valid foreign intelligence target had remained tasked [redacted] while the target was in the United States from [redacted] by a second analyst, upon learning of the target's visit. At that time, however, the second analyst was not aware [redacted]

(b) (1)
(b) (3) - P.L. 86-36

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 3024(i)

The first analyst immediately detasked the selector [redacted] and deleted the query and the results the following day. Both analysts were counseled on the proper procedures for ensuring that all selectors associated with a target are detasked.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an auditor discovered that an analyst had performed a query in an [redacted] of a raw traffic database on a selector known to be a USP. Upon being told of the mistake, the analyst immediately deleted the query and the results.

(b) (1)
(b) (3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an analyst mistakenly queried on a selector associated with a USP as a result of not being familiar with the new functionality provided by the query form. The analyst realized her mistake immediately and deleted the query and the results.

~~(TS//SI//NF)~~ [redacted] analysts performed queries on selectors associated with a USP in a raw traffic database without conducting the necessary research on the selectors. The queries and the results were deleted.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] it was discovered that [redacted] selectors associated with [redacted] valid foreign intelligence targets had [redacted] while the target was in the United States. [redacted] the analyst had detasked the selector [redacted]. All results have been deleted.

(b) (1)
(b) (3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an auditor discovered that, on [redacted] query in an FAA §702 raw traffic database using [redacted] selectors associated with a known USP. [redacted] the query and the results were deleted. No reports were issued.

(b) (1)
(b) (3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an analyst discovered [redacted] selectors associated with an individual who was not the intended target and who had traveled to the United States. A [redacted] selector that was correctly associated with the intended target was queried when the target was in the United States.

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 3024(i)

I.B.4.a.iv (U) Detasking Delays

~~(TS//SI//NF)~~ [redacted] it was discovered that [redacted] potentially causing a delay in detasking of up to 24 hours on some requests. [redacted] detask selectors immediately upon request.

~~(TS//SI//NF)~~ [redacted] it was discovered that [redacted] Upon discovery of the error, the selectors were immediately detasked and the non-compliant data was marked for purging.

(b) (1)
(b) (3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] it was discovered that selectors associated with valid foreign intelligence targets had remained on task while the targets

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

were in the United States. [redacted] the targets were in the United States. The selectors were detasked and all non-compliant data were marked for purging.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] it was discovered that [redacted] the foreign intelligence target selector had remained on task while the target was in the United States. The selector was detasked [redacted] Non-compliant data has been marked for purging.

(b) (1)
(b) (3) - P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] it was discovered that [redacted] selectors associated with a foreign intelligence target had remained on task while the target was in the United States from [redacted] The delay occurred because a junior analyst was unaware of the detasking procedures. The selectors were not detasked because the target returned to a foreign location [redacted] All non-compliant data from [redacted] has been marked for purging.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] it was discovered that [redacted] selectors associated with valid foreign intelligence targets had remained on task when the targets arrived in the United States. On each occasion, the analyst [redacted] The selectors were detasked, and all non-compliant data was purged. No reports were issued.

(b) (1)
(b) (3) - P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] it was discovered that selectors associated with [redacted] valid foreign intelligence targets had remained on task when the targets were in the United States. [redacted] The selectors were detasked upon discovery of the incidents, and all non-compliant data was purged. No reports were issued.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] it was discovered that a selector associated with a valid foreign intelligence target had remained on task while the target was in the United States. [redacted] All non-compliant data was purged.

(b) (1)
(b) (3) - P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an analyst discovered that a selector associated with a valid foreign intelligence target had remained on task when the target arrived in the United States [redacted] The analyst believed that he had detasked the selector at that time, but it actually had remained on task [redacted] All non-compliant data was purged, and no reports were issued.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] it was discovered that a selector associated with a valid foreign intelligence target had remained on task while the target was in the United States from [redacted] The selector remained tasked because the target had returned to a foreign location. The non-compliant data was purged.

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an analyst discovered that a selector associated with a valid foreign intelligence target had remained on task when the target visited the United States from [redacted]. When the analyst was originally notified that [redacted] his target was in the United States [redacted] the analyst initiated a detasking, but the detasking was not executed. When the analyst was notified a second time [redacted] that the target was located in the United States, the selector was immediately detasked. All non-compliant data was purged.

(b) (1)
(b) (3) - P.L. 86-36

~~(TS//SI//NF)~~ [redacted] NSA analysts discovered that a selector had remained on task because of a software error [redacted]. The system error was corrected [redacted]. Non-compliant data has been marked for purging.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] it was discovered that [redacted] selectors associated with [redacted] valid foreign intelligence targets had remained on task while the target was in the United States. The selectors were detasked and the non-compliant data was purged.

~~(TS//SI//NF)~~ [redacted] an analyst discovered that [redacted] selectors associated with a valid foreign intelligence target had remained on task while the target was visiting the United States from [redacted]. The analyst was aware on [redacted] that the target was in the United States and believed that the selectors had been detasked that day. [redacted] the analyst realized that the selectors had not been detasked but did not request the selectors to be detasked at that time because the target had returned to a foreign location. All non-compliant data was purged, and no reports were issued.

(b) (1)
(b) (3) - P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an analyst discovered that [redacted] collection had occurred on [redacted] selectors associated with a valid foreign intelligence target visiting the United States. [redacted]. The collection occurred because the [redacted] the selectors were detasked and the non-compliant data was purged. No reports were issued.

(b) (1)
(b) (3) - P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an analyst discovered that [redacted] selectors associated with a valid foreign intelligence target had remained on task when the target was in the United States. [redacted] resulting in collection of the target while in the United States. The selectors were detasked and the non-compliant data was purged.

(b) (1)
(b) (3) - P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] it was discovered that a selector associated with valid foreign intelligence target had remained on task while the target was in the United States. [redacted]. The selectors were not detasked because the target had returned to a foreign location. All non-compliant data has been marked for purging.

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] it was discovered that selectors associated with valid foreign intelligence targets had remained on task while the targets were in the United States. [redacted]

[redacted] All the selectors were detasked, and the non-compliant data was marked for purging.

I.B.4.a.v. (U) Data-Handling Errors

(b) (1)

(b) (3) - P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an analyst sent an e-mail, which included an attachment with FAA §702 data, to an IC analyst not authorized to receive it. Upon discovery, the recipient deleted the e-mail without opening the attachment. The analyst was counseled on proper data-handling procedures.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an analyst sent an e-mail, which included an attachment with FAA §702 data, to three analysts not authorized to receive it. Upon discovery, the recipients deleted the e-mail and the file to which the information was downloaded.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] it was discovered that analysts were storing FAA §702 data in directories without controlling access to the information. The analysts were using outdated guidance and were unaware of the proper procedures for handling FAA §702 data. The analysts were informed of the proper procedures, and the data was placed in proper directories.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an analyst discovered that software failed to place FAA §702 data in the proper file directory that would have provided access controls. Instead, the placement of the FAA §702 defaulted to a directory that could be accessed by unauthorized and untrained personnel, although highly unlikely. [redacted] changes to the software were made to ensure the proper placement of FAA §702 data.

~~(S//REL TO USA, FVEY)~~ [redacted] it was discovered that [redacted] an analyst had shared FAA §702 data with a second analyst not authorized to receive it. Upon discovery, access to the data was discontinued until the second analyst received the proper training on handling FAA §702 data.

I.B.4.a.vi. (U) Unauthorized Access

(b) (1)

(b) (3) - P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] a supervisor discovered that a [redacted] analyst was accessing FAA §702 data from an unauthorized location. The analyst was approved for FAA §702 data access but then transferred to another location on [redacted] at which time her access should have been terminated. Upon discovery of the incident, the analyst's access to FAA §702 was discontinued.

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an analyst discovered that another analyst was accessing FAA §702 data from an unauthorized location. The analyst was approved for FAA §702 data access [redacted] but then transferred to another location in

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

[redacted] at which time her access should have been terminated. Upon discovery of the incident, the analyst's access to FAA §702 was discontinued.

(b) (1)
(b) (3)-P.L. 86-36

I.B.4.a.vii (U) Systems Error

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 3024(i)

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

[redacted]

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

[redacted]

I.B.4.b. (U) FAA Section 704

(U) Section 704 of the FISA provides for the targeting of United States persons located outside the United States pursuant to a particularized court order.

I.B.4.b.i. (U) Detasking Delays

~~(TS//SI//NF)~~ [redacted] it was discovered that selectors for a FAA §704-approved target had remained on task [redacted]

[redacted] The selectors were detasked [redacted]

(b) (1)
(b) (3)-P.L. 86-36

I.B.4.c. (U) FAA Section 705(b)

(U) Section 705(b) of the FISA provides for the targeting of United States persons located outside the United States upon authorization by the Attorney General when court orders have been obtained authorizing a physical search or electronic surveillance.

I.B.4.c.i. (U) Database Queries

~~(TS//SI//NF)~~ [redacted] a database auditor discovered that an analyst had performed [redacted] queries on an FAA §705-approved target [redacted]

(b) (1)
(b) (3)-P.L. 86-36

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

[redacted]

~~(TS//SI//NF)~~ [redacted] an analyst was notified by [redacted] that a target tasked under FAA §705(b) authority had returned to the United States [redacted]

(b) (1)
(b) (3)-P.L. 86-36

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 3024(i)

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

The selector was detasked [redacted] To prevent future detasking delays. NSA analysts reminded [redacted] of the necessity to [redacted] FAA §705(b) targets.

I.C. (U) Consensual Collection

(b) (1)

(b) (3) - P.L. 86-36

(U) Nothing to report.

I.D. (U) Dissemination of U.S. Identities

~~(TS//SI//NF)~~ The NSA/CSS enterprise issued [redacted] SIGINT product reports during the fourth quarter of CY2012. In [redacted] product reports, disseminations were found to be improper, and the reports were recalled as NSA/CSS and [redacted] analysts learned of USPs, U.S. organizations, or U.S. entities named without authorization. All data in the recalled reports was deleted as required, and the reports were not re-issued or were re-issued with proper minimization.

I.E. (U) Counterintelligence Activities

(U) Nothing to report.

I.F. (U) Detection and Prevention of Violations

~~(TS//SI//NF)~~ As previously reported, NSA has instituted a process to help identify when the users of properly tasked [redacted] the United States. NSA's telephony process identified [redacted] in the fourth quarter. Collected data was purged from NSA/CSS's raw traffic repositories. NSA's process for [redacted] [redacted] in the fourth quarter. Collected data was purged from NSA/CSS's raw traffic repositories.

I.G. (U) Other

(b) (3) - P.L. 86-36

(b) (1)

(b) (3) - P.L. 86-36

(U//~~FOUO~~) In [redacted] instances, database accesses were not terminated when analysts were deployed or reassigned to another site. Although not considered violations of E.O. 12333 or related directives, the accesses were terminated in accordance with NSA policy. In addition, there was [redacted] instance of unauthorized access to raw SIGINT and [redacted] instances of account sharing during the quarter.

II. (U) NSA/CSS Office of the Inspector General (OIG) Intelligence Oversight (IO) Inspections, Investigations, and Special Studies

(U//~~FOUO~~) During the fourth quarter of CY2012, the OIG reviewed various NSA/CSS intelligence activities to determine whether they had been conducted in accordance with statutes, E.O.s, AG-approved procedures, and Department of Defense and internal directives. The problems uncovered were routine and the reviews showed that operating elements understand the restrictions on NSA/CSS activities.

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~II.A. ~~(S//REL TO USA, FVEY)~~ [REDACTED]

~~(S//REL TO USA, FVEY)~~ During the field inspection of [REDACTED] an IO inspector reviewed IO program management, IO training provided to personnel assigned to the site, and procedures for ensuring that all site personnel received required IO training. The inspector's overall assessment was that the site had a rudimentary IO program that needed further documentation and development. The OIG recommended that the site document its IO processes and procedures and conduct informal IO training sessions for site personnel.

II.B. (U) **Special Study of the Research Directorate's (RD) Compliance Program**

(U//~~FOUO~~) The NSA OIG summarized the results of a review of the NSA RD's Compliance Program in a report published [REDACTED]. The review, conducted [REDACTED] focused on the operation of the program by the Directorate's IO component. The review identified two areas of improvement for the IO compliance program: program documentation and enhanced controls to monitor IO training compliance for the RD workforce.

II.C. (U) **Special Study: Assessment of Management Controls Over FAA §702**

(b) (3)-P.L. 86-36

(U//~~FOUO~~) The NSA OIG reported the results of a review of the management controls implemented to provide reasonable assurance of compliance with FAA §702. The report, published [REDACTED] identified one instance of non-compliance and included recommendations to improve the overall control environment in which FAA §702 authority is exercised. Information received after the report's issuance that had not been made available to the OIG during the initial review indicated that there had been no instance of non-compliance and that the control procedures are designed to comply with FAA §702.

II.D. (U) **Advisory Report on [REDACTED] Compliance with NSA/CSS Authorities**

(U//~~FOUO~~) [REDACTED] the NSA OIG conducted a review of [REDACTED] a technology demonstration that uses cloud computing. In an advisory report published [REDACTED] the OIG found that controls on data ingestion and on [REDACTED] participants required manual implementation to comply with NSA/CSS authorities, leaving [REDACTED] compliance measures vulnerable to human error. Furthermore, these controls were not sustainable outside the tightly controlled [REDACTED] environment.

(b) (3)-P.L. 86-36

II.E. (U) **Ongoing Studies**

(U//~~FOUO~~) The following special studies were initiated during the quarter and will be summarized in subsequent quarterly reports:

- (U//~~FOUO~~) FAA §702 [REDACTED]
- (U) Special Study: Assessment of Management Controls Over FAA §702 – Revision
- (U) Special Study of [REDACTED] Auditing Control Framework for Signals Intelligence System Queries

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

(b) (3) - P.L. 86-36

- (U) Special Study of the [] System
- (U) Special Study of the Technology Directorate Mission Compliance Program
- (U) Special Study of the Information Assurance Directorate Office of Oversight and Compliance Mission Compliance Program

II.F. (U) Misuse of the U.S. SIGINT System

(U) Nothing to report

II.G. (U) Congressional and IO Board Notifications

~~(S//SI//NF)~~ [] NSA notified the Congressional intelligence (b) (1) committees about a Title I FISA compliance incident involving the misapplication of certain (b) (3) - P.L. 86-36 provisions of NSA's minimization procedures. After learning of one instance in which domestic communications encountered in the course of authorized collection had not been handled as required, senior NSA managers initiated a full-scale review. Although the review is ongoing, they have learned that there was no indication of willful non-compliance of minimization procedures; personnel seem to have misapplied those procedures. Retraining sessions are ongoing.

II.H. (U) Other Notifications

~~(TS//SI//NF)~~ The AG granted NSA/CSS approval for [] intelligence-related collection activities associated with USP hostage and detainee cases.

III. (U) Substantive Changes to the NSA/CSS IO Program

(b) (1)

(b) (3) - P.L. 86-36

A. (U) []

~~(U//FOUO)~~ As reported in the Second Quarter CY2011 report, NSA/CSS is developing a tool designed to automate the process of submitting mission compliance incident reports across the worldwide NSA/CSS enterprise. The [] will become the Agency's central tool for (b) (3) - P.L. 86-36 reporting all potential mission compliance incidents and will provide such benefits as a streamlined management process, a central repository, and metrics data to support root cause identification and trend analysis. The [] is expected to be implemented [] With the implementation of the [] NSA will be able to perform comprehensive trend analysis []

IV. (U) Changes to NSA/CSS Published Directives or Policies Concerning Intelligence, Counterintelligence, or Intelligence-Related Activities and the Reason for the Changes

(U) Nothing to report.

V. (U) Procedures Governing the Activities of DoD Intelligence Components that Affect USP (DoD Directive 5240.1-R, Procedure 15) Inquiries or Matters Related to IO Programs~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

(U) Nothing to report.

VI. (U) Crimes Reporting

(U) Nothing to Report

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 3024(i)

VII. (U) Other Matters

~~(S//NF)~~ The NSA OIG is continuing its investigation into an allegation reported in the Third Quarter CY2012 report that [redacted]

[redacted]

~~(TS//SI//NF)~~

[redacted]

[redacted]

[redacted] NSA verbally notified the Office of the Assistant to the Secretary of Defense for Intelligence Oversight of this issue.

(U) NSA/CSS has taken the following remedial actions:

- ~~(S//NF)~~ NSA/CSS has obtained approval from the Undersecretary of Defense for Intelligence [redacted]

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-50 USC 3024(i)

- ~~(S//NF)~~ NSA/CSS is working with the [redacted]

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

(U//~~FOUO~~) NSA/CSS does not anticipate that this [redacted] will have any effect on national security or international relations.

~~TOP SECRET//SI//TALENT KEYHOLE//NOFORN~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~



UNITED STATES SIGNALS INTELLIGENCE DIRECTIVE

USSID SP0018

(U) LEGAL COMPLIANCE AND U.S. PERSONS MINIMIZATION PROCEDURES

ISSUE DATE: 25 January 2011

REVISED DATE:

(U) OFFICE OF PRIMARY CONCERN (OPC)

National Security Agency/Central Security Service (NSA/CSS),
Signals Intelligence Directorate (SID), Office of General Counsel

(U) LETTER OF PROMULGATION, ADMINISTRATION, AND AUTHORIZATION

(U) Topic of Promulgation

(U) USSID SP0018 prescribes policies and procedures and assigns responsibilities to ensure that the missions and functions of the United States SIGINT System (USSS) are conducted in a manner that safeguards the constitutional rights of U.S. persons. This USSID delineates and promulgates the USSS minimization policy and procedures required to protect the privacy

Approved for release by the National Security Agency on 13 November 2013, FOIA Case #71241

Derived From: NSA/CSSM I-52

Declassified

~~SECRET//SI//REL TO USA, FVEY~~

EXHIBIT
AEX16

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

rights of U.S. persons.

-
- (U) USSID Edition (U) This USSID supersedes USSID SP0018, dated 27 July 1993, which must now be destroyed.
-
- (U) Legal Protection of Sensitive Information (U//~~FOUO~~) This USSID contains sensitive information that is legally protected from public disclosure and is to be used only for official purposes of National Security Agency/Central Security Services (NSA/CSS).
-
- (U) Handling of USSID (U//~~FOUO~~) Users must strictly adhere to all classification and handling restrictions (see NSA/CSS Classification Manual 1-52) when:
- (U) storing hard or soft copies of this USSID, or
 - (U) hyperlinking to this USSID.
- (U) Users are responsible for the update and management of this USSID when it is stored locally.
-
- (U) Location of Official USSID (U//~~FOUO~~) The SIGINT Policy System Manager will maintain and update the current official USSID on NSANet. As warranted, the USSID will be available on INTELINK.
-
- (U) Access by Contractors and Consultants (U) For NSA elements to include the SIGINT Extended Enterprise:
- (U//~~FOUO~~) USSS contractors or consultants assigned to NSA/CSS Headquarters or to other elements of the SIGINT Extended Enterprise are pre-authorized for access to USSIDs via NSANet, Intelink, or in hard-copy formats as needed to perform their jobs. However, for those sensitive USSIDs for which access is password-controlled, all users, to include contractors, must undergo additional security and mission vetting.
- (U) Outside NSA elements:
- (U//~~FOUO~~) Non-USSS contractors or consultants working at external facilities are pre-authorized for soft-copy access to USSIDs via NSANet or in selected cases, via INTELINK, if connectivity to those systems is allowed by the contractor's NSA/CSS sponsor. Where such connectivity is not established, any hard-copy provision of USSIDs must be authorized by the SIGINT Policy System Manager (NSTS: 966-5487, STE: DSN:)
-
- (U) Access by Third Party (U) This USSID is not releasable to any Third Party partner.

(b)(3)-P.L. 86-36

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

Partners

(U) If a shareable version of this USSID is requested:

- (U) refer to USSID SP0002, Annex B, and
- (U) contact the appropriate Country Desk Officer in the Foreign Affairs Directorate.

(U) Executive Agent

(U) The Executive Agent for this USSID is:

//s/

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

(U) TABLE OF CONTENTS

(U) Sections

SECTION 1 - (U) PREFACE

SECTION 2 - (U) REFERENCES

SECTION 3 - (U) POLICY

SECTION 4 - (U) COLLECTION

SECTION 5 - (U) PROCESSING

SECTION 6 - (U) RETENTION

SECTION 7 - (U) DISSEMINATION

SECTION 8 - (U) RESPONSIBILITIES

SECTION 9 - (U) DEFINITIONS

(U) Annexes and Appendices

ANNEX A - (U) PROCEDURES IMPLEMENTING TITLE I OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

APPENDIX 1 - (U//~~FOUO~~) STANDARD MINIMIZATION PROCEDURES FOR ELECTRONIC SURVEILLANCE CONDUCTED BY THE NATIONAL SECURITY AGENCY (NSA)

ANNEX B - (U) OPERATIONAL ASSISTANCE TO THE FEDERAL BUREAU OF INVESTIGATION

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

ANNEX C - (U) SIGNALS INTELLIGENCE SUPPORT TO U.S. AND ALLIED MILITARY EXERCISE COMMAND AUTHORITIES

ANNEX D - (U) TESTING OF ELECTRONIC EQUIPMENT

ANNEX E - (U) SEARCH AND DEVELOPMENT OPERATIONS

ANNEX F - (U) ILLICIT COMMUNICATIONS

ANNEX G - (U) TRAINING OF PERSONNEL IN THE OPERATION AND USE OF SIGINT COLLECTION AND OTHER SURVEILLANCE EQUIPMENT

ANNEX H - (U) CONSENT FORMS

ANNEX I - (U) FORM FOR CERTIFICATION OF OPENLY ACKNOWLEDGED ENTITIES

ANNEX J - ~~(S//REL)~~ PROCEDURES FOR MONITORING RADIO COMMUNICATIONS OF SUSPECTED INTERNATIONAL NARCOTICS TRAFFICKERS *(Issued Separately)*

ANNEX K - ~~(S//REL)~~ [REDACTED]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

SECTION 1 - (U) PREFACE

(U) Fourth Amendment Protections

1.1. (U) The Fourth Amendment to the United States Constitution protects all U.S. persons anywhere in the world and all persons within the United States from unreasonable searches and seizures by any person or agency acting on behalf of the U.S. Government. The Supreme Court has ruled that the interception of electronic communications is a search and seizure within the meaning of the Fourth Amendment. It is therefore mandatory that signals intelligence (SIGINT) operations be conducted pursuant to procedures which meet the reasonableness requirements of the Fourth Amendment.

(U) Balancing Foreign Intelligence Need and Privacy Interest

1.2. (U) In determining whether United States SIGINT System (USSS) operations are "reasonable," it is necessary to balance the U.S. Government's need for foreign intelligence information and the privacy interests of persons protected by the Fourth Amendment. Striking that balance has consumed much time and effort by all branches of the United States Government. The results of that effort are reflected in the references listed in Section 2 below. Together, these references require the minimization of U.S. person information collected, processed, retained or disseminated by the USSS. The purpose of this document

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

is to implement these minimization requirements.

1.3. (U) Several themes run throughout this USSID. The most important is that intelligence operations and the protection of constitutional rights are not incompatible. It is not necessary to deny legitimate foreign intelligence collection or suppress legitimate foreign intelligence information to protect the Fourth Amendment rights of U.S. persons.

(U) Minimization of U.S. Person Information

1.4. (U) These minimization procedures implement the constitutional principle of "reasonableness" by giving different categories of individuals and entities different levels of protection. These levels range from the stringent protection accorded U.S. citizens and permanent resident aliens in the United States to provisions relating to foreign diplomats in the U.S. These differences reflect yet another main theme of these procedures, that is, that the focus of all foreign intelligence operations is on foreign entities and persons.

(U) Oversight Functions

1.5. (U) Nothing in these procedures shall restrict the performance of lawful compliance or oversight functions over the USSS.

SECTION 2 - (U) REFERENCES**(U) References**

2.1 (U) The following documents are references to this USSID:

- (U) 50 U.S.C. 1801, et seq., Foreign Intelligence Surveillance Act (FISA) of 1978, as amended.
- (U) Executive Order 12333, "United States Intelligence Activities," as amended 30 July 2008.
- (U) (U) DoD Directive 5240.01, "DoD Intelligence Activities," dated 27 August 2007.
- (U) NSA/CSS Policy No. 1-23, "Procedures Governing NSA/CSS Activities that affect U.S. Persons," as revised 29 May 2009.
- (U) DoD Regulation 5240.1-R, "Procedures Governing the Activities of DoD Intelligence Components that Affect United States Person," dated December 1982.

SECTION 3 - (U) POLICY**(U) Policy and the USSS Foreign**

3.1. (U) The policy of the USSS is to TARGET or COLLECT only FOREIGN COMMUNICATIONS.* The USSS will not intentionally COLLECT

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

Communications Mission communications to, from or about U.S. PERSONS or persons or entities in the U.S. except as set forth in this USSID. If the USSS inadvertently COLLECTS such communications, it will process, retain and disseminate them only in accordance with this USSID.

* (U) Capitalized words in Sections 3 through 9 are defined terms in Section 9.

SECTION 4 - (U) COLLECTION

(U) Collection 4.1. ~~(S//SI//REL)~~ Communications which are known to be to, from or about a U.S. PERSON [redacted] not be intentionally intercepted, or selected through the use of a SELECTION TERM, except in the following instances:

(b)(1)

a. ~~(U//FOUO)~~ With the approval of the United States Foreign Intelligence Surveillance Court either under the conditions outlined in Annex A of this USSID or as permitted by other FISA authorities.

b. (U) With the approval of the Attorney General of the United States, if

(1) (U) The COLLECTION is directed against the following:

(a) ~~(U//FOUO)~~ Communications to or from U.S. PERSONS outside the UNITED STATES if such persons have been approved for targeting in accordance with the terms of FISA (e.g., the targeted U.S. PERSON is the subject of an order or authorization issued pursuant to Sections 105, 703, 704, or 705(b) of FISA), or

(b) ~~(S//SI//REL)~~ International communications to, from,

[redacted]

(b)(1)

(c) ~~(U//FOUO)~~ Communications which are not to or from but merely about U.S. PERSONS (wherever located).

(2) (U) The person is an AGENT OF A FOREIGN POWER, and

(3) (U) The purpose of the COLLECTION is to acquire significant FOREIGN INTELLIGENCE information.

c. ~~(U//FOUO)~~ With the approval of the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS), so long as the COLLECTION need not be approved by the Foreign Intelligence Surveillance Court or the Attorney General, and

~~SECRET//SI//REL TO USA, FVEY~~

~~SECRET//SI//REL TO USA, FVEY~~

(1) (U//~~FOUO~~) The person has CONSENTED to the COLLECTION by executing one of the CONSENT forms contained in Annex H, or

(2) (U//~~FOUO~~) The person is reasonably believed to be held captive by a FOREIGN POWER or group engaged in INTERNATIONAL TERRORISM, or

(3) (~~S//REL~~) The TARGETED [redacted] and the DIRNSA/CHCSS has approved the COLLECTION in accordance with Annex I, or

(b)(1)

(4) (~~S//SI//REL~~) The COLLECTION is directed against [redacted] between a U.S. PERSON in the UNITED STATES and a foreign entity outside the UNITED STATES, the TARGET is the foreign entity, and the DIRNSA/CHCSS has approved the COLLECTION in accordance with Annex K, or

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(f)
(b)(3)-18 USC 798

(5) (~~S//SI//REL~~) Technical devices (e.g., [redacted]) are employed to limit acquisition by the USSS to communications to or from the TARGET or to specific forms of communications used by the TARGET (e.g., [redacted]) and the COLLECTION is directed against [redacted] voice and facsimile communications with one COMMUNICANT in the UNITED STATES, and the TARGET of the COLLECTION is [redacted]

(b)(1)

(a) A non-U.S. PERSON located outside the UNITED STATES [redacted]

(b) [redacted]

(6) (U//~~FOUO~~) Copies of approvals granted by the DIRNSA/CHCSS under these provisions will be retained in the Office of General Counsel for review by the Attorney General.

d. (U) Emergency Situations:

(1) (U//~~FOUO~~) Unless separate authorization under FISA is required by law, I in emergency situations DIRNSA/CHCSS may

1 (U//~~FOUO~~) Collection that constitutes "electronic surveillance" as defined by FISA can only be authorized in accordance with the terms of FISA. Under certain circumstances, the Attorney General may authorize emergency collection that constitutes "electronic surveillance" under FISA. For purposes of FISA, the term

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

authorize the COLLECTION of information to, from, or about a U.S. PERSON who is outside the UNITED STATES when securing the prior approval of the Attorney General is not practical because:

(a) (U) The time required to obtain such approval would result in the loss of significant FOREIGN INTELLIGENCE and would cause substantial harm to the national security.

(b) (U) A person's life or physical safety is reasonably believed to be in immediate danger.

(c) (U) The physical security of a defense installation or government property is reasonably believed to be in immediate danger.

(2) (U//~~FOUO~~) In those cases where the DIRNSA/CHCSS authorizes emergency COLLECTION, except for actions taken under paragraph d.(1)(b) above, DIRNSA/CHCSS shall find that there is probable cause that the TARGET meets one of the following criteria:

(a) (U) A person who, for or on behalf of a FOREIGN POWER, is engaged in clandestine intelligence activities (including covert activities intended to affect the political or governmental process), sabotage, or INTERNATIONAL TERRORIST activities, or activities in preparation for INTERNATIONAL TERRORIST activities; or who conspires with, or knowingly aids and

"electronic surveillance" encompasses 1) the acquisition by an electronic, mechanical, or other surveillance device the contents of any wire or radio communications sent by or intended to be received by a particular, known, United States person if the contents are acquired by intentionally targeting the U.S. person under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, absent the U.S. person's express or implied consent, 2) the acquisition by electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States, but does not include those communications of computer trespassers that would be permissible under section 2511(2)(i) of title 18 of the United States Code, 3) the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required if the acquisition were undertaken for law enforcement purposes, and if both the sender and all intended recipients are located inside the United States, or 4) the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required if the acquisition were undertaken for law enforcement purposes.

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

abets a person engaging in such activities.

(b) (U) A person who is an officer or employee of a FOREIGN POWER.

(c) (U) A person unlawfully acting for, or pursuant to the direction of, a FOREIGN POWER. The mere fact that a person's activities may benefit or further the aims of a FOREIGN POWER is not enough to bring that person under this subsection, absent evidence that the person is taking direction from, or acting in knowing concert with, the FOREIGN POWER.

(d) (U) A CORPORATION or other entity that is owned or controlled directly or indirectly by a FOREIGN POWER.

(e) (U) A person in contact with, or acting in collaboration with, an intelligence or security service of a foreign power for the purpose of providing access to information or material classified by the United States to which such person has access.

(3) (U) In all cases where emergency collection is authorized, the following steps shall be taken:

(a) (U//~~FOUO~~) The General Counsel will be notified immediately that the COLLECTION has started.

(b) (U//~~FOUO~~) The General Counsel will initiate immediate efforts to obtain Attorney General approval to continue the collection. If Attorney General approval is not obtained within 72 hours, the COLLECTION will be terminated. If the Attorney General approves the COLLECTION, it may continue for the period specified in the approval.

e. (U//~~FOUO~~) Annual reports to the Attorney General are required for COLLECTION conducted under paragraphs 4.1.c.(3) and (4). Responsible analytic offices will provide such reports through the Signals Intelligence Director and the General Counsel (GC) to the DIRNSA/CHCSS for transmittal to the Attorney General by 31 January of each year.

~~SECRET//SI//REL TO USA, FVEY~~

~~SECRET//SI//REL TO USA, FVEY~~

(U) [redacted] 4.2. (S//SI//REL) [redacted]
[redacted]

a. (S//SI//REL) [redacted]
[redacted]

(b)(1)

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

b. (S//SI//REL) [redacted]
[redacted]

(U) Incidental Acquisition of U.S. Person Information

4.3. (U) Information to, from or about U.S. PERSONS acquired incidentally as a result of COLLECTION directed against appropriate FOREIGN INTELLIGENCE TARGETS may be retained and processed in accordance with Section 5 and Section 6 of this USSID.

(U) Nonresident Alien Targets

4.4. (S//SI//REL) Nonresident Alien TARGETS Entering the UNITED STATES.

a. (S//SI//REL) If the communications of a nonresident alien located abroad are being TARGETED and the USSS learns that the individual has entered the UNITED STATES, COLLECTION may continue for a period of 72 hours provided that continued COLLECTION is otherwise permitted by FISA.2 the DIRNSA/CHCSS is advised immediately, and:

(1) Immediate efforts are initiated to obtain Attorney General approval, or

(2) A determination is made within the 72 hour period that the

[redacted]

(b)(1)

b. (U) If Attorney General approval is obtained, the COLLECTION may

2 (S//SI//REL) There is no 72 hour grace period for collection that has been authorized pursuant to Sections 702, 703, 704, or 705(b) of FISA. Collection under Sections 702, 703, 704, or 705(b) of FISA must be terminated as soon as the USSS learns the target has entered the United States. Similarly, DIRNSA may not authorize use of a collection technique while the target is located inside the United States if use of the collection technique would qualify as "electronic surveillance" under FISA (see Footnote 1).

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

continue for the length of time specified in the approval.

c. (U//~~FOUO~~) If it is determined that [REDACTED] [REDACTED] COLLECTION may continue at the discretion of the operational element.

(b)(1)

d. (S//SI//REL) If [REDACTED] or if Attorney General approval is not obtained within 72 hours, COLLECTION must be terminated [REDACTED] Attorney General approval is obtained, or the individual leaves the UNITED STATES.

(U//~~FOUO~~) U.S. Person Targets4.5. (U//~~FOUO~~) U.S. PERSON TARGETS Entering the UNITED STATES.

a. (U//~~FOUO~~) If communications to, from or about a U.S. PERSON located outside the UNITED STATES are being COLLECTED under Court or Attorney General approval as described in Sections 4.1 a. and 4.1.b. above, the COLLECTION must stop when the USSS learns that the individual has entered the UNITED STATES.

b. (U//~~FOUO~~) While the individual is in the UNITED STATES, COLLECTION may be resumed only with the approval of the United States Foreign Intelligence Surveillance Court as described in Annex A.

4.6. (S//REL) Requests to TARGET U.S. PERSONS. All proposals for COLLECTION against U.S. PERSONS, [REDACTED] [REDACTED] must be submitted through the Signals Intelligence Director and the GC to the DIRNSA/CHCSS for review.

(b)(1)

(U) Direction Finding

4.7. (U//~~FOUO~~) Use of direction finding solely to determine the location of a transmitter located outside of the UNITED STATES does not constitute ELECTRONIC SURVEILLANCE or COLLECTION even if directed at transmitters believed to be used by U.S. PERSONS. Unless COLLECTION of the communications is otherwise authorized under these procedures, the contents of communications to which a U.S. PERSON is a party monitored in the course of direction finding may only be used to identify the transmitter.

(U) Distress Signals

4.8. (U) Distress signals may be intentionally collected, processed, retained, and disseminated without regard to the restrictions contained in this USSID.

(U) Automated Information Systems

4.9. (U) COMSEC Monitoring and Security Testing of Automated Information Systems. Monitoring for communications security purposes must be conducted with the consent of the person being monitored and in accordance with the

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

procedures established in National Telecommunications and Information Systems Security Directive 600, Communications Security (COMSEC) Monitoring, dated 10 April 1990. Monitoring for communications security purposes is not governed by this USSID. Intrusive security testing to assess security vulnerabilities in automated information systems likewise is not governed by this USSID.

SECTION 5- (U) PROCESSING

(U) Selection Terms 5.1. (~~S//SI//REL~~) Use of Selection Terms During Processing. When a SELECTION TERM is intended to INTERCEPT a communication on the basis of the content of the communication, or because a communication is enciphered, rather than on the basis of the identity of the COMMICANT or the fact that the communication mentions a particular individual, the following rules apply:

a. (~~S//SI//REL~~) No SELECTION TERM that is reasonably likely to result in the INTERCEPTION of communications to or from a U.S. PERSON (wherever located), [REDACTED] (b)(1)
[REDACTED] may be used unless there is reason to believe that FOREIGN INTELLIGENCE will be obtained by use of such SELECTION TERM.

b. (U//~~FOUO~~) No SELECTION TERM that has resulted in the INTERCEPTION of a significant number of communications to or from such persons or entities may be used unless there is reason to believe that FOREIGN INTELLIGENCE will be obtained.

c. (U//~~FOUO~~) SELECTION TERMS that have resulted or are reasonably likely to result in the INTERCEPTION of communications to or from such persons or entities shall be designed to defeat, to the greatest extent practicable under the circumstances, the INTERCEPTION of those communications which do not contain FOREIGN INTELLIGENCE.

5.2. (U//~~FOUO~~) Annual Review by the Signals Intelligence Director:

a. (U//~~FOUO~~) All SELECTION TERMS that are reasonably likely to result in the INTERCEPTION of communications to or from a U.S. PERSON or terms that have resulted in the INTERCEPTION of a significant number of such communications shall be reviewed annually by the Signals Intelligence Director or a designee.

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET-SECRET TO USA, FVEY~~

b. (U//~~FOUO~~) The purpose of the review shall be to determine whether there is reason to believe that FOREIGN INTELLIGENCE will be obtained, or will continue to be obtained, by the use of these SELECTION TERMS.

c. (U//~~FOUO~~) A copy of the results of the review will be provided to the Inspector General (IG) and the GC.

**(U) Intercepted
Material**

5.3. (U) Forwarding of Intercepted Material. FOREIGN COMMUNICATIONS collected by the USSS may be forwarded as intercepted to NSA, intermediate processing facilities, and collaborating centers.

5.4. (U) Non-foreign Communications.

a. (U) Communications between persons in the UNITED STATES. Private communications solely between persons in the UNITED STATES inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be promptly destroyed unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

b. (U) Communications between U.S. PERSONS. Communications solely between U.S. PERSONS will be treated as follows:

(1) (U) Communications solely between U.S. PERSONS inadvertently intercepted during the COLLECTION of FOREIGN COMMUNICATIONS will be destroyed upon recognition, if technically possible, except as provided in paragraph 5.4.d. below.

(2) (U) Notwithstanding the preceding provision, cryptologic data (e.g., signal and encipherment information) and technical communications data (e.g., circuit usage) may be extracted and retained from those communications if necessary to:

(a) (U) Establish or maintain intercept, or

(b) (U) Minimize unwanted intercept, or

(c) (U) Support cryptologic operations related to FOREIGN COMMUNICATIONS.

c. (U) Communications Involving an Officer or Employee of the U.S. Government. Communications to or from any officer or employee of

~~SECRET-SECRET TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

the U.S. Government, or any state or local government, will not be intentionally intercepted. Inadvertent INTERCEPTIONS of such communications (including those between foreign TARGETS and U.S. officials) will be treated as indicated in paragraphs 5.4.a. and b., above.

d. (U) Exceptions: Notwithstanding the provisions of paragraphs 5.4.b. and c., the DIRNSA/CHCSS may waive the destruction requirement for international communications containing, inter alia, the following types of information:

- (1) Significant FOREIGN INTELLIGENCE, or
- (2) Evidence of a crime or threat of death or serious bodily harm to any person, or
- (3) Anomalies that reveal a potential vulnerability to U.S. communications security. Communications for which the Attorney General or DIRNSA/CHCSS's waiver is sought should be forwarded to NSA/CSS, Attn: Signals Intelligence Directorate Office of Oversight & Compliance (SV).

**(U) Radio
Communications**

5.5. (U) Radio Communications with a Terminal in the UNITED STATES

a. ~~(S//SI//REL)~~ All radio communications that pass over channels with a terminal in the UNITED STATES must be processed through a computer scan dictionary or similar device unless those communications occur over channels used exclusively by a FOREIGN POWER.

b. ~~(S//SI//REL)~~ International common-access radio communications that pass over channels with a terminal in the UNITED STATES, other than communications, may be processed without the use of a computer scan dictionary or similar device if necessary to determine whether a channel contains communications of FOREIGN INTELLIGENCE interest which NSA may wish to collect. Such processing may not exceed two hours without the specific prior written approval of the Signals Intelligence Director or a designee and, in any event, shall be limited to the minimum amount of time necessary to determine the nature of communications on the channel and the amount of such communications that include FOREIGN INTELLIGENCE. Once it is determined that the channel contains sufficient communications of FOREIGN INTELLIGENCE interest to warrant COLLECTION and exploitation to produce FOREIGN INTELLIGENCE, a computer scan dictionary or similar device must be used for additional processing.

c. (U//~~FOUO~~) Copies of all written approvals made pursuant to 5.5.b. must be provided to the GC and the IG.

~~SECRET//SI//REL TO USA, FVEY~~

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

~~SECRET//SI//REL TO USA, FVEY~~

SECTION 6- (U) RETENTION

(U) Retention of Communications**6.1. (U) Retention of Communications to, from or About U.S. PERSONS.**

a. (U) Except as otherwise provided in Annex A, Appendix 1, Section 4, communications to, from or about U.S. PERSONS that are intercepted by the USSS may be retained in their original or transcribed form only as follows:

(1) (U//~~FOUO~~) Unenciphered communications not thought to contain secret meaning may be retained for five years unless the Signals Intelligence Director determines in writing that retention for a longer period is required to respond to authorized FOREIGN INTELLIGENCE requirements.

(2) (U//~~FOUO~~) Communications necessary to maintain technical data bases for cryptanalytic or traffic analytic purposes may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future FOREIGN INTELLIGENCE requirement. Sufficient duration may vary with the nature of the exploitation and may consist of any period of time during which the technical data base is subject to, or of use in, cryptanalysis. If a U.S. PERSON'S identity is not necessary to maintaining technical data bases, it should be deleted or replaced by a generic term when practicable.

b. (U) Communications which could be disseminated under Section 7, below (i.e., without elimination of references to U.S. PERSONS) may be retained in their original or transcribed form.

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

- (U) Access 6.2. (U) Access to raw traffic storage systems which contain identities of U.S. PERSONS must be limited to SIGINT production personnel or other persons who conduct signals intelligence activities under the direction, authority, or control of DIRNSA/CHCSS. For more information on access to SIGINT, refer to USSID CRJ610, 2.3.

SECTION 7- (U) DISSEMINATION

- (U) Focus of SIGINT Reports 7.1. (U) All SIGINT reports will be written so as to focus solely on the activities of foreign entities and persons and their agents. Except as provided in Section 7.2., FOREIGN INTELLIGENCE information concerning U.S. PERSONS must be disseminated in a manner which does not identify the U.S. PERSON. Generic or general terms or phrases must be substituted for the identity (e.g., "U.S. firm" for the specific name of a U.S. CORPORATION or "U.S. PERSON" for the specific name of a U.S. PERSON). Files containing the identities of U.S. persons deleted from SIGINT reports will be maintained for a maximum period of one year and any requests from SIGINT customers for such identities should be referred to the Signals Intelligence Directorate's Office of Information Sharing Services (S12).

- (U) Dissemination of U.S. PERSON Identities 7.2. (U) SIGINT reports may include the identification of a U.S. PERSON only if one of the following conditions is met and a determination is made by the appropriate approval authority that the recipient has a need for the identity for the performance of his official duties:

a. (U) The U.S. PERSON has CONSENTED to the dissemination of communications of, or about, him or her and has executed the CONSENT form found in Annex H of this USSID, or

b. (U) The information is PUBLICLY AVAILABLE (i.e., the information is derived from unclassified information available to the general public), or

c. (U) The identity of the U.S. PERSON is necessary to understand the FOREIGN INTELLIGENCE information or assess its importance. The following nonexclusive list contains examples of the type of information that meet this standard:

(1) (U) FOREIGN POWER or AGENT OF A FOREIGN POWER. The information indicates that the U.S. PERSON is a FOREIGN POWER or an AGENT OF A FOREIGN POWER.

(2) (U) Unauthorized Disclosure of Classified Information. The

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

information indicates that the U.S. PERSON may be engaged in the unauthorized disclosure of classified information.

(3) (U) International Narcotics Activity. The information indicates that the individual may be engaged in international narcotics trafficking activities. (See Annex J of this USSID for further information concerning individuals involved in international narcotics trafficking).

(4) (U) Criminal Activity. The information is evidence that the individual may be involved in a crime that has been, is being, or is about to be committed, provided that the dissemination is for law enforcement purposes.

(5) (U) Intelligence TARGET. The information indicates that the U.S. PERSON may be the TARGET of hostile intelligence activities of a FOREIGN POWER.

(6) (U) Threat to Safety. The information indicates that the identity of the U.S. PERSON is pertinent to a possible threat to the safety of any person or organization, including those who are TARGETS, victims or hostages of INTERNATIONAL TERRORIST organizations. Reporting units shall identify to S12 any report containing the identity of a U.S. PERSON reported under this subsection (6). Field reporting to S12 should be in the form of a CRITICOMM message and include the report date-time-group (DTG), product serial number and the reason for inclusion of the U.S. PERSON'S identity.

(7) (U) Senior Executive Branch Officials. The identity is that of a senior official of the Executive Branch of the U.S. Government. In this case only the official's title will be disseminated. Domestic political or personal information on such individuals will be neither disseminated nor retained.

(U) Approval Authorities

7.3. (U) Approval authorities for the release of identities of U.S. persons under Section 7 are as follows:

a. (U) DIRNSA/CHCSS. DIRNSA/CHCSS must approve dissemination of:

(1) The identities of any senator, congressman, officer, or employee of the Legislative Branch of the U.S. Government.

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

(2) The identity of any person for law enforcement purposes.

b. (U) Field Units and NSA Headquarters Elements. All SIGINT production organizations are authorized to disseminate the identities of U.S. PERSONS when:

(1) The identity is pertinent to the safety of any person or organization;

(2) The identity is that of a senior official of the Executive Branch; or

(3) The U.S. PERSON has CONSENTED under paragraph 7.2.a. above.

c. (U) Signals Intelligence Director and Designees.

(1) In all other cases, U.S. PERSON identities may be released only with the prior approval of the Signals Intelligence Director, the Deputy Signals Intelligence Director, the Chief, S12, the Deputy Chief, S12, or the Senior Operations Officer of the National Security Operations Center.

(2) For law enforcement purposes involving narcotics related information, DIRNSA has granted to the Signals Intelligence Director authority to disseminate U.S. identities. This authority may not be further delegated.

(U) Privileged Communications and Criminal Activity

7.4. (U) Privileged Communications and Criminal Activity. All proposed disseminations of information constituting U.S. PERSON privileged communications (e.g., attorney/client, doctor/patient) and all information concerning criminal activities or criminal or judicial proceedings in the UNITED STATES must be reviewed by the Office of General Counsel prior to dissemination.

(U) Improper Dissemination

7.5. (U) If the name of a U.S. PERSON is improperly disseminated, the incident should be reported to S12 and SV within 24 hours of discovery of the error.

SECTION 8 - (U) RESPONSIBILITIES

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~(U) Inspector
General

8.1. (U) The Inspector General shall:

- a. (U) Conduct regular inspections and perform general oversight of NSA/CSS activities to ensure compliance with this USSID.
- b. (U) Establish procedures for reporting by NSA/CSS signals intelligence elements of their activities and practices for oversight purposes.
- c. (U) Report to the DIRNSA/CHCSS, annually by 31 October, concerning NSA/CSS compliance with this USSID.
- d. (U) Report quarterly with the DIRNSA/CHCSS and General Counsel to the President's Intelligence Oversight Board through the Assistant to the Secretary of Defense (Intelligence Oversight).

(U) General
Counsel

8.2. (U) The General Counsel shall:

- a. (U) Provide legal advice and assistance to all elements of the USSS regarding SIGINT activities. Requests for legal advice on any aspect of these procedures may be sent by CRITICOMM, secure email, or by NSA/CSS, secure telephone 963-3121, STE or non-secure (301) 688-5015. (b)(3)-P.L. 86-36
- b. (U) Prepare and process all applications for Foreign Intelligence Surveillance Court orders and requests for Attorney General approvals required by these procedures.
- c. (U) Advise the IG in inspections and oversight of USSS activities.
- d. (U) Review and assess for legal implications as requested by the DIRNSA/CHCSS, Deputy Director, IG, Signals Intelligence Director, or their designees, all new major requirements and internally generated USSS activities.
- e. (U) Advise USSS personnel of new legislation and case law that may affect USSS missions, functions, operations, activities, or practices.
- f. (U) Report as required to the Attorney General and the President's Intelligence Oversight Board and provide copies of such reports to the DIRNSA/CHCSS and affected agency elements.
- g. (U) Process requests from any DoD intelligence component for authority to use signals as described in Procedure 5, Part 5, of DoD 5240.1-R, for periods in excess of 90 days in the development, test, or calibration of ELECTRONIC SURVEILLANCE equipment and other equipment that can intercept communications.

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~**(U) Signals
Intelligence
Director**

8.3. (U) The Signals Intelligence Director shall:

- a. (U) Ensure that all SIGINT production personnel understand and maintain a high degree of awareness and sensitivity to the requirements of this USSID.
- b. (U) Apply the provisions of this USSID to all SIGINT production activities. The Signals Intelligence Directorate staff focal point for USSID SP0018 (formerly USSID 18) matters is SV.
- c. (U) Conduct necessary reviews of SIGINT production activities and practices to ensure consistency with this USSID.
- d. (U) Ensure that all new major requirements levied on the USSS or internally generated activities are considered for review by the GC. All activities that raise questions of law or the proper interpretation of this USSID must be reviewed by the GC prior to acceptance or execution.

**(U) All Elements
of the USSS**

8.4. (U) All elements of the USSS shall:

- a. (U) Implement this directive upon receipt.
- b. (U) Prepare new procedures or amend or supplement existing procedures as required to ensure adherence to this USSID. A copy of such procedures shall be forwarded to NSA/CSS, Attn: SV.
- c. (U) Immediately inform the Signals Intelligence Director of any tasking or instructions that appear to require actions at variance with this USSID.
- d. (U) Promptly report to the NSA IG and consult with the NSA GC on all activities that may raise a question of compliance with this USSID.

SECTION 9 - (U) DEFINITIONS

**(U) Agent of
Foreign Power**

9.1. (U) AGENT OF A FOREIGN POWER means:

- a. (U) Any person, other than a U.S. PERSON, who:

- (1) (U) Acts in the UNITED STATES as an officer or employee of a FOREIGN POWER, or as a member of a group engaged in INTERNATIONAL TERRORISM or activities in preparation therefore; or

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET-SECRET TO USA, FVEY~~

(2) (U) Acts for, or on behalf of, a FOREIGN POWER that engages in clandestine intelligence activities in the UNITED STATES contrary to the interests of the UNITED STATES, when the circumstances of such person's presence in the UNITED STATES indicate that such person may engage in such activities in the UNITED STATES, or when such person knowingly aids or abets any person in the conduct of such activities or knowingly conspires with any person to engage in such activities; or

b. (U) Any person, including a U.S. PERSON, who:

(1) (U) Knowingly engages in clandestine intelligence gathering activities for, or on behalf of, a FOREIGN POWER, which activities involve, or may involve, a violation of the criminal statutes of the UNITED STATES; or

(2) (U) Pursuant to the direction of an intelligence service or network of a FOREIGN POWER, knowingly engages in any other clandestine intelligence activities for, or on behalf of, such FOREIGN POWER, which activities involve or are about to involve, a violation of the criminal statutes of the UNITED STATES; or

(3) (U) Knowingly engages in sabotage or INTERNATIONAL TERRORISM, or activities that are in preparation thereof, for or on behalf of a FOREIGN POWER; or

(4) (U) Knowingly aids or abets any person in the conduct of activities described in paragraphs 9.1.b. (1) through (3) or knowingly conspires with any person to engage in those activities.

c. (U) For all purposes other than the conduct of ELECTRONIC SURVEILLANCE as defined by the Foreign Intelligence Surveillance Act (see Annex A), the phrase "AGENT OF A FOREIGN POWER" also means any person, including U.S. PERSONS outside the UNITED STATES, who are officers or employees of a FOREIGN POWER, or who act unlawfully for or pursuant to the direction of a FOREIGN POWER, or who are in contact with or acting in collaboration with an intelligence or security service of a FOREIGN POWER for the purpose of providing access to information or material classified by the UNITED STATES Government and to which the person has or has had access. The mere fact that a person's activities may benefit or further the aims of a FOREIGN POWER is not enough to bring that person under this provision, absent evidence that the person is taking direction from or acting in knowing concert with a FOREIGN POWER.

(U) Collection

9.2. (U) COLLECTION means intentional tasking or SELECTION of

~~SECRET-SECRET TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

identified nonpublic communications for subsequent processing aimed at reporting or retention as a file record.

-
- (U) Communicant** 9.3. (U) COMMUNICANT means a sender or intended recipient of a communication.
-
- (U) Communications about a U.S. Person** 9.4. (U) COMMUNICATIONS ABOUT A U.S. PERSON are those in which the U.S. PERSON is identified in the communication. A U.S. PERSON is identified when the person's name, unique title, address, or other personal identifier is revealed in the communication in the context of activities conducted by that person or activities conducted by others and related to that person. A mere reference to a product by brand name or manufacturer's name, e.g., "Boeing 707" is not an identification of a U.S. person.
-
- (U) Consent** 9.5. (U) CONSENT, for SIGINT purposes, means an agreement by a person or organization to permit the USSS to take particular actions that affect the person or organization. An agreement by an organization with the National Security Agency to permit COLLECTION of information shall be deemed valid CONSENT if given on behalf of such organization by an official or governing body determined by the GC, National Security Agency, to have actual or apparent authority to make such an agreement.
-
- (U) Corporations** 9.6. (U) CORPORATIONS, for purposes of this USSID, are entities legally recognized as separate from the persons who formed, own, or run them. CORPORATIONS have the nationality of the nation state under whose laws they were formed. Thus, CORPORATIONS incorporated under UNITED STATES federal or state law are U.S. PERSONS.
-
- (U) Electronic Surveillance** 9.7. (U) ELECTRONIC SURVEILLANCE means:
- a. (U) In the case of an electronic communication, the acquisition of a nonpublic communication by electronic means without the CONSENT of a person who is a party to the communication.
 - b. (U) In the case of a nonelectronic communication, the acquisition of a nonpublic communication by electronic means without the CONSENT of a person who is visibly present at the place of communication.
 - c. (U) The term ELECTRONIC SURVEILLANCE does not include the use of radio direction finding equipment solely to determine the location of a transmitter.

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

(U) Foreign Communication 9.8. (U) FOREIGN COMMUNICATION means a communication that has at least one COMMICANT outside of the UNITED STATES, or that is entirely among FOREIGN POWERS or between a FOREIGN POWER and officials of a FOREIGN POWER, but does not include communications intercepted by ELECTRONIC SURVEILLANCE directed at premises in the UNITED STATES used predominantly for residential purposes.

(U) Foreign Intelligence 9.9. (U) FOREIGN INTELLIGENCE means information relating to the capabilities, intentions, and activities of FOREIGN POWERS, organizations, or persons, and for purposes of this USSID includes both positive FOREIGN INTELLIGENCE and counterintelligence

(U) Foreign Power 9.10. (U) FOREIGN POWER means:

- a. (U) A foreign government or any component thereof, whether or not recognized by the UNITED STATES.
- b. (U) A faction of a foreign nation or nations, not substantially composed of UNITED STATES PERSONS.
- c. (U) An entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments.
- d. (U) A group engaged in INTERNATIONAL TERRORISM or activities in preparation thereof.
- e. (U) A foreign-based political organization, not substantially composed of UNITED STATES PERSONS, or
- f. (U) An entity that is directed and controlled by a foreign government or governments

(U) Interception 9.11. (U) INTERCEPTION means the acquisition by the USSS through electronic means of a nonpublic communication to which it is not an intended party, and the processing of the contents of that communication into an intelligible form, but does not include the display of signals on visual display devices intended to permit the examination of the technical characteristics of the signals without reference to the information content carried by the signal.

(U) International Terrorism 9.12. (U) INTERNATIONAL TERRORISM means activities that:

- a. (U) Involve violent acts or acts dangerous to human life that are a

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

violation of the criminal laws of the UNITED STATES or of any State, or that would be a criminal violation if committed within the jurisdiction of the UNITED STATES or any State, and

b. (U) Appear to be intended:

(1) (U) to intimidate or coerce a civilian population,

(2) (U) to influence the policy of a government by intimidation or coercion, or

(3) (U) to affect the conduct of a government by assassination or kidnapping, and

c. (U) Occur totally outside the UNITED STATES, or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum.

(U) Publicly Available Information

9.13. (U) PUBLICLY AVAILABLE INFORMATION means information that has been published or broadcast for general public consumption, is available on request to a member of the general public, has been seen or heard by a casual observer, or is made available at a meeting open to the general public.

(U) Selection

9.14. (~~S//SI//REL~~) SELECTION, as applied to manual and electronic processing activities, means the intentional insertion of a [redacted] telephone number, email address, [redacted] into a computer scan dictionary or manual scan guide for the purpose of identifying messages of interest and isolating them for further processing.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

(U) Selection Term

9.15. (U//~~FOUO~~) SELECTION TERM means the composite of individual terms used to effect or defeat SELECTION of particular communications for the purpose of INTERCEPTION. It comprises the entire term or series of terms so used, but not any segregable term contained therein. It applies to both electronic and manual processing.

(U) Target

9.16. (U) TARGET, OR TARGETING: See COLLECTION.

(U) United States

9.17. (U) UNITED STATES, when used geographically, includes the 50 states and the District of Columbia, Puerto Rico, Guam, American Samoa, the U.S. Virgin Islands, the Northern Mariana Islands, and any other territory or

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

possession over which the UNITED STATES exercises sovereignty.

(U) United States Person 9.18. (U) UNITED STATES PERSON:

- a. (U) A citizen of the UNITED STATES.
- b. (U) An alien lawfully admitted for permanent residence in the UNITED STATES.
- c. (U) Unincorporated groups and associations a substantial number of the members of which constitute a. or b. above, or
- d. (U) CORPORATIONS incorporated in the UNITED STATES, including U.S. flag nongovernmental aircraft or vessels, but not including those entities which are openly acknowledged by a foreign government or governments to be directed and controlled by them.
- e. (U) The following guidelines apply in determining whether a person is a U.S. PERSON:

(1) (U) A person known to be currently in the United States will be treated as a U.S. PERSON unless that person is reasonably identified as an alien who has not been admitted for permanent residence or if the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is not a U.S. PERSON.

(2) (U) A person known to be currently outside the UNITED STATES, or whose location is not known, will not be treated as a U.S. PERSON unless such person is reasonably identified as such or the nature of the person's communications or other indicia in the contents or circumstances of such communications give rise to a reasonable belief that such person is a U.S. PERSON.

(3) (U) A person known to be an alien admitted for permanent residence may be assumed to have lost status as a U.S. PERSON if the person leaves the UNITED STATES and it is known that the person is not in compliance with the administrative formalities provided by law (8 U.S.C. Section 1203) that enable such persons to reenter the UNITED STATES without regard to the provisions of law that would otherwise restrict an alien's entry into the UNITED STATES. The failure to follow the statutory procedures provides a reasonable basis to conclude that such alien has abandoned any intention of maintaining status as a permanent resident alien.

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

(4) (U) An unincorporated association whose headquarters are located outside the UNITED STATES may be presumed not to be a U.S. PERSON unless the USSS has information indicating that a substantial number of members are citizens of the UNITED STATES or aliens lawfully admitted for permanent residence.

(5) (U) CORPORATIONS have the nationality of the nation/state in which they are incorporated. CORPORATIONS formed under U.S. federal or state law are thus U.S. persons, even if the corporate stock is foreign-owned. The only exception set forth above is CORPORATIONS which are openly acknowledged to be directed and controlled by foreign governments. Conversely, CORPORATIONS incorporated in foreign countries are not U.S. PERSONS even if that CORPORATION is a subsidiary of a U.S. CORPORATION.

(6) (U) Nongovernmental ships and aircraft are legal entities and have the nationality of the country in which they are registered. Ships and aircraft fly the flag and are subject to the law of their place of registration.

USSID SP0018

ANNEX A - (U) PROCEDURES IMPLEMENTING TITLE I OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT

SECTION 1 - (U) PURPOSE AND APPLICABILITY

(U) Foreign
Intelligence
Surveillance Act

A1.1. (U) Title I of the Foreign Intelligence Surveillance Act (the Act) governs the conduct of certain electronic surveillance activities within the United States to collect foreign intelligence information.

A1.2. (U) Title I of the Act covers the intentional collection of the communications of a particular, known U.S. person who is in the United States.

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

all wiretaps in the United States, the acquisition of certain radio communications where all parties to that communication are located in the United States, and the monitoring of information in which there is a reasonable expectation of privacy.

A1.3. (U) The Act requires that all such surveillances be directed only at foreign powers and their agents as defined by the Act and that all such surveillances be authorized by the United States Foreign Intelligence Surveillance Court, or in certain limited circumstances, by the Attorney General.

SECTION 2 - (U) GENERAL

(U) PROCEDURE AND STANDARDS

A2.1. (U) Procedures and standards for securing Court orders or Attorney General certifications to conduct electronic surveillances are set forth in the Act. Requests for such orders or certifications should be forwarded by the appropriate Key Component through the NSA GC to the DIRNSA/CHCSS and should be accompanied by a statement of the facts and circumstances justifying a belief that the target is a foreign power or an agent of a foreign power and that each of the facilities or places at which the surveillance will be directed are being used, or are about to be used, by that foreign power or agent.

A2.2. (U) If the proposed surveillance meets the requirements of the Act and the Director approves the proposal, attorneys in the OGC will draw the necessary court application or request for Attorney General certification.

SECTION 3 - (U) MINIMIZATION PROCEDURES

(U) Surveillances

A3.1. (U//~~FOUO~~) Surveillances authorized by the Act are required to be carried out in accordance with the Act and pursuant to the court order or Attorney General certification authorizing that particular surveillance. In some cases, the court orders are tailored to address particular problems, and in those instances the NSA attorney will advise the appropriate NSA offices of the terms of the court's orders. In most cases, however, the court order will incorporate without any changes the standardized minimization procedures set forth in Appendix I.

SECTION 4 - (U) RESPONSIBILITIES

(U) General Counsel Responsibilities

A4.1. (U) The GC will review all requests to conduct electronic surveillances as defined by the Act, prepare all applications and materials required by the Act, and provide pertinent legal advice and assistance to all elements of the United

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

States SIGINT System.

(U) Inspector
General
Responsibilities

A4.2. (U) The IG will conduct regular inspections and oversight of all SIGINT activities to assure compliance with this Directive.

(U) SIGINT
Manager and
Supervisor
Responsibilities

A4.3. (U) All SIGINT managers and supervisors with responsibilities relating to the Act will ensure that they and their personnel are thoroughly familiar with the Act, its implementing procedures, and any court orders or Attorney General certifications pertinent to their mission. Personnel with duties related to the Act will consult the GC's office for any required legal advice and assistance or training of newly assigned personnel.

A4.4. (U) Appropriate records will be maintained demonstrating compliance with the terms of all court orders and Attorney General certifications, and any discrepancies in that regard will be promptly reported to the offices of the GC and IG.

USSID SP0018, ANNEX A

APPENDIX 1 - (U) STANDARD MINIMIZATION PROCEDURES FOR ELECTRONIC SURVEILLANCE CONDUCTED BY THE NATIONAL SECURITY AGENCY (NSA)

UNITED STATES

FOREIGN INTELLIGENCE SURVEILLANCE COURT

WASHINGTON, D.C.

STANDARD MINIMIZATION

PROCEDURES FOR ELECTRONIC SURVEILLANCE

CONDUCTED BY THE NATIONAL SECURITY AGENCY (NSA)

Pursuant to Section 101(h) of the Foreign Intelligence Surveillance Act of 1978 (hereinafter "the Act"), the following procedures have been adopted by the Attorney General and shall be followed by the NSA in implementing this electronic surveillance: (U)

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~SECTION 1 - APPLICABILITY AND SCOPE (U)

These procedures apply to the acquisition, retention, use, and dissemination of non-publicly available information concerning unconsenting United States persons that is collected in the course of electronic surveillance as ordered by the United States Foreign Intelligence Surveillance Court under Section 102(b) or authorized by Attorney General Certification under Section 102(a) of the Act. These procedures also apply to non-United States persons where specifically indicated. (U)

SECTION 2 - DEFINITIONS (U)

In addition to the definitions in Section 101 of the Act, the following definitions shall apply to these procedures:

(a) Acquisition means the collection by NSA through electronic means of a nonpublic communication to which it is not an intended party. (U)

(b) Communications concerning a United States person include all communications in which a United States person is discussed or mentioned, except where such communications reveal only publicly available information about the person. (U)

(c) Communications of a United States person include all communications to which a United States person is a party. (U)

(d) Consent is the agreement by a person or organization to permit the NSA to take particular actions that affect the person or organization. To be effective, consent must be given by the affected person or organization with sufficient knowledge to understand the action that may be taken and the possible consequences of that action. Consent by an organization shall be deemed valid if given on behalf of the organization by an official or governing body determined by the General Counsel, NSA, to have actual or apparent authority to make such an agreement. (U)

(e) Foreign communication means a communication that has at least one communicant outside of the United States, or that is entirely among:

- (1) foreign powers;
- (2) officers and employees of foreign powers; or
- (3) a foreign power and officers or employees of a foreign power.

All other communications are domestic communications. ~~(S//CCO)~~

(f) Identification of a United States person means the name, unique title, address, or other personal identifier of a United States person in the context of activities conducted by that person or activities conducted by others that are related to that person. A reference to a product by brand name, or manufacturer's name or the use of a name in a descriptive sense, e.g., "Monroe Doctrine," is not an identification of a United States person. ~~(S//CCO)~~

(g) Processed or processing means any step necessary to convert a communication into an intelligible form intended for human inspection. (U)

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

(h) Publicly available information means information that a member of the public could obtain on request, by research in public sources, or by casual observation. (U)

(i) Technical data base means information retained for cryptanalytic, traffic analytic, or signal exploitation purposes. ~~(S-CCO)~~

(j) United States person means a United States person as defined in the Act. The following guidelines apply in determining whether a person whose status is unknown is a United States person: (U)

(1) A person known to be currently in the United States will be treated as a United States person unless positively identified as an alien who has not been admitted for permanent residence, or unless the nature or circumstances of the person's communications give rise to a reasonable belief that such person is not a United States person. (U)

(2) A person known to be currently outside the United States, or whose location is unknown, will not be treated as a United States person unless such person can be positively identified as such, or the nature or circumstances of the person's communications give rise to a reasonable belief that such person is a United States person. (U)

(3) A person known to be an alien admitted for permanent residence loses status as a United States person if the person leaves the United States and is not in compliance with Title 8, United States Code, Section 1203 enabling re-entry into the United States. Failure to follow the statutory procedures provides a reasonable basis to conclude that the alien has abandoned any intention of maintaining his status as a permanent resident alien. (U)

(4) An unincorporated association whose headquarters or primary office is located outside the United States is presumed not to be a United States person unless there is information indicating that a substantial number of its members are citizens of the United States or aliens lawfully admitted for permanent residence. (U)

SECTION 3 - ACQUISITION AND PROCESSING - GENERAL (U)

(a) Acquisition (U)

The acquisition of information by electronic surveillance shall be made in accordance with the certification of the Attorney General or the court order authorizing such surveillance and conducted in a manner designed, to the greatest extent reasonably feasible, to minimize the acquisition of information not relevant to the authorized purpose of the surveillance. ~~(S-CCO)~~

(b) Verification (U)

At the initiation of the electronic surveillance, the NSA or the Federal Bureau of Investigation, if providing operational support, shall verify that the communication lines or telephone numbers being targeted are the lines or numbers of the target authorized by court order or Attorney General certification. Thereafter, collection personnel will monitor the acquisition of raw data at regular intervals to verify that the surveillance is not avoidably acquiring communications outside the authorized scope of the surveillance or information concerning United States persons not related to the purpose of the surveillance. ~~(S-CCO)~~

(c) Monitoring, Recording, and Processing (U)

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

(1) Electronic surveillance of the target may be monitored contemporaneously, recorded automatically, or both (U)

(2) Personnel who monitor the electronic surveillance shall exercise reasonable judgement in determining whether particular information acquired must be minimized and shall destroy inadvertently acquired communications of or concerning a United States person at the earliest practicable point in the processing cycle at which such communication can be identified either as clearly not relevant to the authorized purpose of the surveillance (i.e., the communication does not contain foreign intelligence information) or as containing evidence of a crime which may be disseminated under these procedures. ~~(S-CCO)~~

(3) Communications of or concerning United States persons that may be related to the authorized purpose of the surveillance may be forwarded to analytic personnel responsible for producing intelligence information from the collected data. Such communications or information may be retained and disseminated only in accordance with Sections 4, 5, and 6 of these procedures. ~~(C)~~

(4) Magnetic tapes or other storage media that contain acquired communications may be processed. ~~(S-CCO)~~

(5) Each communication shall be reviewed to determine whether it is a domestic or foreign communication to or from the targeted premises and is reasonably believed to contain foreign intelligence information or evidence of a crime. Only such communications may be processed. All other communications may be retained or disseminated only in accordance with Sections 5 and 6 of these procedures. ~~(S-CCO)~~

(6) Magnetic tapes or other storage media containing foreign communications may be scanned by computer to identify and select communications for analysis. Computer selection terms used for scanning, such as telephone numbers, key words or phrases, or other discriminators, shall not include United States person names or identifiers and shall be limited to those selection terms reasonably likely to identify [redacted]

[redacted] that are authorized for intentional collection under Executive Order 12333 implementing procedures. ~~(S-CCO)~~

(b)(1)

(7) Further processing, retention and dissemination of foreign communications shall be made in accordance with Sections 4, 6, and 7, as applicable, below. Further processing, storage and dissemination of inadvertently acquired domestic communications shall be made in accordance with Sections 4 and 5 below. ~~(S-CCO)~~

(d) U.S. Persons Employed by the Foreign Power ~~(C)~~

Communications of or concerning United States persons employed by a foreign power may be used and retained as otherwise provided in these procedures except that:

(1) Such United States persons shall not be identified in connection with any communication that the person places or receives on behalf of another unless the identification is permitted under Section 6 of these procedures; and

(2) personal communications of United States persons that could not be foreign intelligence may only be retained, used, or disseminated in accordance with Section 5 of these procedures. ~~(S-CCO)~~

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

(e) Destruction of Raw Data ~~(C)~~

Communications and other information, including that reduced to graphic or "hard copy" form such as [redacted] shall be reviewed for retention in accordance with the standards set forth in these procedures. Communications and other information, in any form, that do not meet

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

such retention standards and that are known to contain communications of or concerning United States persons shall be promptly destroyed. ~~(S-CCO)~~

(f) Non-pertinent Communications (U)

(1) Communications determined to fall within established categories of non-pertinent communications, such as those set forth in subparagraph (6) of this section, should not be retained unless they contain information that may be disseminated under Sections 5, 6, or 7 below. (U)

(2) Monitors may listen to all communications, including those that initially appear to fall within established categories until they can reasonably determine that the communication cannot be disseminated under Sections 5, 6, or 7 below. ~~(S-CCO)~~

(3) Communications of United States persons will be analyzed to establish categories of communications that are not pertinent to the authorized purpose of the surveillance. (U)

(4) These categories should be established after a reasonable period of monitoring the communications of the targets. (U)

(5) Information that appears to be foreign intelligence may be retained even if it is acquired as a part of a communication falling within a category that is generally non-pertinent. ~~(S-CCO)~~

(6) Categories of non-pertinent communications which may be applied in these surveillance include:

(A) Calls to and from United States Government officials;

(B) Calls to and from children;

(C) Calls to and from students for information to aid them in academic endeavors;

(D) Calls between family members; and

(E) Calls relating solely to personal services, such as food orders, transportation, etc. ~~(S-CCO)~~

(g) Change in Target's Location or Status ~~(S-CCO)~~

(1) During periods of known extended absence by a targeted agent of a foreign power from premises under surveillance, only communications to which the target is a party may be retained and disseminated. ~~(S-CCO)~~

(2) When there is reason to believe that the target of an electronic surveillance is no longer a foreign power or an agent of a foreign power, or no longer occupies the premises authorized for surveillance, that electronic surveillance shall be immediately terminated, and shall not resume unless subsequently approved under the Act. When any person involved in collection or processing of an electronic surveillance being conducted pursuant to the Act becomes aware of information tending to indicate a material change in the status or location of a target, the person shall immediately ensure that the NSA's Office of General Counsel is also made aware of such information. ~~(S-CCO)~~

SECTION 4 - ACQUISITION AND PROCESSING - SPECIAL PROCEDURES (U)

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

~~SECRET//SI//REL TO USA, FVEY~~

(a) Collection Against Residential Premises ~~(S-CCO)~~

(b)(1)

(1) An electronic surveillance directed against premises located in the United States and used for residential purposes shall be conducted by technical means designed to limit the information acquired to communications that have one communicant outside the United States. [redacted]

[redacted] The technical means employed shall consist of [redacted] equipment or equipment capable of identifying international [redacted] or other particular international communications known to be used by the targeted foreign power and its agents. Communications to or from the target residential premises that are processed [redacted] [redacted] of a foreign power or agent of a foreign power located in a foreign country, or on the foreign country or foreign city telephone direct dialing codes (area codes) for the areas in which such foreign powers or agents are located. ~~(S-CCO)~~

(2)

[redacted]

~~(S-CCO)~~

(3) Domestic communications that are incidentally acquired during collection against residential premises shall be handled under Section 5 of these procedures. ~~(S-CCO)~~

(b) Attorney-Client Communications ~~(S)~~

As soon as it becomes apparent that a communication is between a person who is known to be under criminal indictment and an attorney who represents that individual in the matter under indictment (or someone acting on behalf of the attorney), monitoring of that communication will cease and the communication shall be identified as an attorney-client communication in a log maintained for that purpose. The relevant portion of the tape containing that conversation will be placed under seal and the Department of Justice, Office of Intelligence Policy and Review, shall be notified so that appropriate procedures may be established to protect such communications from review or use in any criminal prosecution, while preserving foreign intelligence information contained therein. ~~(S-CCO)~~

SECTION 5 - DOMESTIC COMMUNICATIONS (U)

(a) Dissemination (U)

Communications identified as domestic communications shall be promptly destroyed, except that:

(1) domestic communications that are reasonably believed to contain foreign intelligence information shall be disseminated to the Federal Bureau of Investigation (including United States person identities) for possible further dissemination by the Federal Bureau of Investigation in accordance with its minimization procedures,

(2) domestic communications that do not contain foreign intelligence information, but that are reasonably believed to contain evidence of a crime that has been, is being, or is about to be committed, shall be disseminated (including United States person identities) to appropriate Federal law enforcement authorities, in accordance with Section 106(b) of the Act and crimes reporting procedures approved by the Secretary of Defense and the Attorney General; and

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

(3) domestic communications that are reasonably believed to contain technical data base information, as defined in Section 2(i), may be disseminated to the Federal Bureau of Investigation and to other elements of the U.S. SIGINT system. ~~(S//CCO)~~

(b) Retention (U)

(1) Domestic communications disseminated to Federal law enforcement agencies may be retained by the NSA for a reasonable period of time, not to exceed six months (or any shorter period set by court order), to permit law enforcement agencies to determine whether access to original recordings of such communications is required for law enforcement purposes. ~~(S//CCO)~~

(2) Domestic communications reasonably believed to contain technical data base information may be retained for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation. ~~(S//CCO)~~

a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis. ~~(S//CCO)~~

b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is one year unless the Deputy Director for Operations, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements. ~~(S//CCO)~~

SECTION 6 - FOREIGN COMMUNICATIONS OF OR CONCERNING UNITED STATES PERSONS

(U)

(a) Retention (U)

Foreign communications of or concerning United States persons acquired by the NSA in the course of an electronic surveillance subject to these procedures may be retained only:

(1) if necessary for the maintenance of technical data bases. Retention for this purpose is permitted for a period sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future foreign intelligence requirement. Sufficient duration may vary with the nature of the exploitation.

a. In the context of a cryptanalytic effort, maintenance of technical data bases requires retention of all communications that are enciphered or reasonably believed to contain secret meaning, and sufficient duration may consist of any period of time during which encrypted material is subject to, or of use in, cryptanalysis.

b. In the case of communications that are not enciphered or otherwise thought to contain secret meaning, sufficient duration is one year unless the Deputy Director for Operations, NSA, determines in writing that retention for a longer period is required to respond to authorized foreign intelligence or counterintelligence requirements.

(2) if dissemination of such communications with reference to such United States persons would be permitted under subsection (b) below, or

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

(3) if the information is evidence of a crime that has been, is being, or is about to be committed and is provided to appropriate federal law enforcement authorities. (~~S-FCO~~)

(b) Dissemination (U)

A report based on communications of or concerning a United States person may be disseminated in accordance with Section 7 if the identity of the United States person is deleted and a generic term or symbol is substituted so that the information cannot reasonably be connected with an identifiable United States person. Otherwise dissemination of intelligence reports based on communications of or concerning a United States person may only be made to a recipient requiring the identity of such person for the performance of official duties but only if at least one of the following criteria is also met:

(1) the United States person has consented to dissemination or the information of or concerning the United States person is available publicly;

(2) the identity of the United States person is necessary to understand foreign intelligence information or assess its importance, e.g., the identity of a senior official in the Executive Branch;

(3) the communication or information indicates that the United States person may be:

(A) an agent of a foreign power;

(B) a foreign power as defined in Section 101(a)(4) or (6) of the Act;

(C) residing outside the United States and holding an official position in the government or military forces of a foreign power

(D) a corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

(E) acting in collaboration with an intelligence or security service of a foreign power and the United States person has, or has had, access to classified national security information or material.

(4) the communication or information indicates that the United States person may be the target of intelligence activities of a foreign power;

(5) the communication or information indicates that the United States person is engaged in the unauthorized disclosure of classified national security information, but only after the agency that originated the information certifies that it is properly classified;

(6) the communication or information indicates that the United States person may be engaging in international terrorist activities;

(7) the acquisition of the United States person's communication was authorized by a court order issued pursuant to Section 105 of the Act and the communication may relate to the foreign intelligence purpose of the surveillance;

(8) the communication or information is reasonably believed to contain evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes and is made in

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA FVEY~~

accordance with Section 106(b) of the Act and crimes reporting procedures approved by the Secretary of Defense and the Attorney General. (U)

SECTION 7 - OTHER FOREIGN COMMUNICATIONS (U)

Foreign communications of or concerning a non-United States person may be retained, used, and disseminated in any form in accordance with other applicable law, regulation, and policy. (U)

SECTION 8 - COLLABORATION WITH FOREIGN GOVERNMENTS (~~S-CCO~~)

(a) The sharing or exchange of foreign communications governed by these procedures with signals intelligence authorities of collaborating foreign governments (Second Parties) may be undertaken by the NSA only with the written assurance of the Second Party that the use of those foreign communications will be subject to the retention and dissemination provisions of these procedures. (~~S-CCO~~)

(b) Domestic communications and communications to or from United States persons shall not be shared with Second Parties. (~~S-CCO~~)

(c) Foreign plain text communications may be shared with Second Parties if they are first reviewed by NSA analysts, who shall remove references to United States persons that are not necessary to understand or assess the foreign intelligence information contained therein. (~~S-CCO~~)

(d) Foreign enciphered or encoded communications may be shared with Second Parties without such prior review, provided that at least annually a representative sampling of those shared communications that can be deciphered or decoded is reviewed by the NSA to ensure that any references therein to United States persons are necessary to understand or assess the foreign intelligence information being disseminated. Corrective measures with respect to each target or line shall be undertaken as necessary to maintain compliance with the above dissemination standard. The results of each review shall be made available to the Attorney General or a designee. (~~S-CCO~~)

Approved by Attorney General Janet Reno on 1 July 1997

~~SECRET//SI//REL TO USA FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~**USSID SP0018****ANNEX B - (U) OPERATIONAL ASSISTANCE TO THE
FEDERAL BUREAU OF INVESTIGATION****SECTION 1 - (U) GENERAL**

(U) Operational Assistance B1.1. (U) In accordance with the provisions of Section 2.6 of E.O. 12333, and the NSA/FBI Memorandum of Understanding of 25 November 1980, the National Security Agency may provide specialized equipment and technical knowledge to the FBI to assist the FBI in the conduct of its lawful functions. When requesting such assistance, the FBI will certify to the General Counsel of NSA/CSS that such equipment or technical knowledge is necessary to the accomplishment of one or more of the FBI's lawful functions.

B1.2. (U) NSA/CSS may also provide expert personnel to assist FBI personnel in the operation or installation of specialized equipment when that equipment is to be employed to collect foreign intelligence. When requesting the assistance of expert personnel, the FBI will certify to the General Counsel that such assistance is necessary to collect foreign intelligence and that the approval of the Attorney General (and, when necessary, a warrant from a court of competent jurisdiction) has been obtained.

SECTION 2 - (U) CONTROL

(U) Operational Control B2.1. (U) No operational assistance as discussed in Section 1 shall be provided without the express permission of the DIRNSA/CHCSS, Deputy Director, NSA/CSS, the SIGINT Director, or the Deputy Director for Technology and Systems. The SIGINT Director and the Director of the Technology Directorate may approve requests for such assistance only with the concurrence of the General Counsel.

USSID SP0018**ANNEX C - (U) SIGNALS INTELLIGENCE SUPPORT TO U.S.
AND ALLIED MILITARY EXERCISE COMMAND
AUTHORITIES**~~SECRET//SI//REL TO USA, FVEY~~

~~SECRET//SI//REL TO USA, FVEY~~

SECTION 1 - (U) POLICY

(U) SIGINT Support

C1.1. (U//~~FOUO~~) Signals Intelligence support to U.S. and Allied military exercise command authorities is provided for in USSID CR1221 and DoD Directive 5200.17 (M-2). Joint Chiefs of Staff Memorandum MJCS111-88, 18 August 1988, and USSID CR1200, 16 December 1988, establish doctrine and procedures for providing signals intelligence support to military commanders. The procedures in this Annex provide policy guidelines for safeguarding the rights of U.S. persons in the conduct of exercise SIGINT support activities.

SECTION 2 - (U) DEFINITIONS

(U) Military Tactical Communi-cations

C2.1. (U) United States and Allied military exercise communications, within the United States and abroad, that are necessary for the production of simulated foreign intelligence and counterintelligence or to permit an analysis of communications security.

SECTION 3 - (U) PROCEDURES

(U) Handling of Military Tactical Communi-cations

C3.1. (U//~~FOUO~~) The USSS may collect, process, store, and disseminate military tactical communications that are also communications of, or concerning, U.S. persons.

a. (U//~~FOUO~~) Collection efforts will be conducted in such a manner as to avoid, to the extent feasible, the intercept of non-exercise-related communications.

b. (U//~~FOUO~~) Military tactical communications may be stored and processed without deletion of references to U.S. persons if the names and communications of the U.S. persons who are exercise participants, whether military, government, or contractor, are contained in, or such communications constitute, exercise-related communications or fictitious communications or information prepared for the exercise.

c. (U//~~FOUO~~) Communications of U.S. persons not participating in the exercise that are inadvertently intercepted during the exercise shall be destroyed as soon as feasible, provided that a record describing the signal or frequency user in technical and generic terms may be retained for signal identification and Collection-avoidance purposes.

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

Inadvertently intercepted communications that contain anomalies in enciphered communications that reveal a potential vulnerability to United States communications security should be forwarded to the Information Assurance Director.

d. (U//~~FOUO~~) Dissemination of military exercise communications, exercise reports, or information files derived from such communications shall be limited to those authorities and persons participating in the exercise or conducting reviews and critiques thereof.

~~SECRET//SI//REL TO USA, FVEY~~

~~SECRET//SI//REL TO USA, FVEY~~**USSID SP0018****ANNEX D - (U) TESTING OF ELECTRONIC EQUIPMENT****SECTION 1 - (U) PURPOSE AND APPLICABILITY****(U) Testing of
Electronic
Equipment**

D1.1. (U) This Annex applies to the testing of electronic equipment that has the capability to intercept communications and other non-public information. Testing includes development, calibration, and evaluation of such equipment, and will be conducted, to the maximum extent practical, without interception or monitoring of U.S. persons.

SECTION 2 - (U) PROCEDURES**(U) Testing
Limitations**

D2.1. (U) The USSS may test electronic equipment that has the capability to intercept communications and other information subject to the following limitations:

a. (U) To the maximum extent practical, the following should be used:

- (1) (U) Laboratory-generated signals;
- (2) (U) Communications transmitted between terminals located outside the United States not used by any known U.S. person;
- (3) (U) Official government agency communications with the consent of an appropriate official of that agency, or an individual's communications with the consent of that individual;
- (4) (U) Public broadcast signals; or
- (5) (U) Other communications in which there is no reasonable expectation of privacy (as approved in each instance by the NSA/CSS General Counsel).

b. (U) Where it is not practical to test electronic equipment solely against signals described in paragraph D2.1.a., above, testing may be conducted, provided:

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

(1) (U) The proposed test is coordinated with the NSA/CSS General Counsel;

(2) (U) The test is limited in scope and duration to that necessary to determine the capability of the equipment;

(3) (U) No particular person is targeted without consent and it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance, and

(4) (U) The test does not exceed 90 calendar days

c. (U) Where the test involves communications other than those identified in paragraph D2.1.a. and a test period longer than 90 days is required, the Foreign Intelligence Surveillance Act requires that the test be approved by the Attorney General. Such proposals and plans shall be submitted by USSS elements through the General Counsel, NSA/CSS, to the DIRNSA/CHCSS for transmission to the Attorney General. The test proposal shall state the requirement for an extended test involving such communications, the nature of the test, the organization that will conduct the test, and the proposed disposition of any signals or communications acquired during the test.

D2.2. (U) The content of any communication other than communications between non-U.S. persons outside the United States which are acquired during a test and evaluation shall be:

a. (U) Retained and used only for the purpose of determining the capability of the electronic equipment;

b. (U) Disclosed only to persons conducting or evaluating the test; and

c. (U) Destroyed before or immediately upon completion of the testing.

D2.3. (U) The technical parameters of a communication, such as frequency, modulation, and time of activity of acquired electronic signals, may be retained and used for test reporting or collection-avoidance purposes. Such parameters may be disseminated to other DoD intelligence components and other entities authorized to conduct electronic surveillance, provided such dissemination and use are limited to testing, evaluation, or collection-avoidance purposes.

USSID SP0018

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~**ANNEX E - (U) SEARCH AND DEVELOPMENT OPERATIONS****SECTION 1 - (U) PROCEDURES****(U) Procedures
for Safeguarding
the Rights of U.S.
Persons**

E1.1. (U) This Annex provides the procedures for safeguarding the rights of U.S. persons when conducting SIGINT search and development activities.

E1.2. (U//~~FOUO~~) The USSS may conduct search and development activities with respect to signals throughout the radio spectrum under the following limitations:

a. (U) Signals may be collected only for the purpose of identifying those signals that:

(1) (U) May contain information related to the production of foreign intelligence or counterintelligence;

(2) (U) Are enciphered or appear to contain secret meaning;

(3) (U) Are necessary to assure efficient signals intelligence collection or to avoid the collection of unwanted signals; or

(4) (~~S//SI//REL~~) Reveal vulnerabilities of United States communications security.

b. (~~S//SI//REL~~) Communications originated or intended for receipt in the United States or originated or intended for receipt by U.S. persons shall be processed in accordance with Section 5 of USSID SP0018, provided that information necessary for cataloging the constituent elements of the signal environment may be processed and retained if such information does not identify a U.S. person. Information revealing a United States communications security vulnerability may be retained.

c. (~~S//SI//REL~~) Information necessary for cataloging the constituent elements of the signal environment may be disseminated to the extent such information does not identify U.S. persons. Communications equipment nomenclature may be disseminated. Information that reveals a vulnerability to United States communications security may be disseminated to the appropriate communications security authorities.

d. (U) All information obtained in the process of search and development that appears to be of foreign intelligence value may be forwarded to the proper analytic office within NSA/CSS for processing and dissemination in accordance with relevant portions of this USSID.

~~SECRET//SI//REL TO USA, FVEY~~

~~SECRET//SI//REL TO USA, FVEY~~

USSID SP0018

ANNEX F - (U) ILLICIT COMMUNICATIONS

SECTION 1 - (U) PROCEDURES

**(U) Handling of
Illicit Communi-
cations**

F1.1. (U) The USSS may collect, retain, process, and disseminate illicit communications without reference to the requirements concerning U.S. persons.

F1.2. (U//~~FOUO~~) The term "illicit communications" means a communication transmitted in violation of either the Communications Act of 1934 and regulations issued thereunder or international agreements, which because of its explicit content, message characteristics, or method of transmission, is reasonably believed to be a communication to or from an agent or agents of foreign powers, whether or not U.S. persons.

USSID SP0018

ANNEX G - (U) TRAINING OF PERSONNEL IN THE OPERATION AND USE OF SIGINT COLLECTION AND OTHER SURVEILLANCE EQUIPMENT

SECTION 1 - (U) APPLICABILITY

(U) Purpose

G1.1. (U) This Annex applies to all USSS use of SIGINT collection and other surveillance equipment for training purposes.

SECTION 2 - (U) POLICY

(U) Training

G2.1. (U) Training of USSS personnel in the operation and use of SIGINT collection equipment shall be conducted, to the maximum extent that is practical, without interception of the communications of U.S. persons or persons in the United States who have not given consent to such interception. Communications and information protected by

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

the Foreign Intelligence Surveillance Act (FISA) (see Annex A) will not be collected for training purposes.

SECTION 3 - (U) PROCEDURES

(U) Training Guidance

G3.1. (U) The training of USSS personnel in the operation and use of SIGINT collection and other surveillance equipment shall include guidance concerning the requirements and restrictions of the FISA, Executive Order 12333, and this USSID.

G3.2. (U) The use of SIGINT collection and other surveillance equipment for training purposes is subject to the following limitations:

a. (U) To the maximum extent practical, use of such equipment for training purposes shall be directed against otherwise authorized intelligence targets.

b. (U) The contents of private communications of nonconsenting U.S. persons may not be acquired unless the person is an authorized target of electronic surveillance, and

c. (U) The electronic surveillance will be limited in extent and duration to that necessary to train personnel in the use of the equipment.

G3.3. (U) The limitations in paragraph G3.2. do not apply in the following instances:

a. (U) Public broadcasts, distress signals, or official United States Government communications may be monitored, provided that, where government agency communications are monitored, the consent of an appropriate official is obtained; and

b. (U) Minimal acquisition of information is permitted as required for calibration purposes.

G3.4. (U) Information collected during training that involves authorized intelligence targets may be retained in accordance with Section 6 of this USSID and disseminated in accordance with Section 7 of this USSID. Information other than distress signals collected during training that does not involve authorized intelligence targets or that is acquired inadvertently shall be destroyed as soon as practical or upon completion of the training and may not be disseminated outside the USSS for any purpose. Distress signals should be referred to the SIGINT Director.

~~SECRET//SI//REL TO USA, FVEY~~

~~SECRET//SI//REL TO USA, FVEY~~**USSID SP0018****ANNEX H - (U) CONSENT FORMS****SECTION 1 - (U) PURPOSE****(U) Forms**

H1.1. (U) The forms set forth in this Annex have been approved by the National Security Agency's Office of General Counsel (NSA OGC) to obtain and record the express consent of a U.S. person for elements of the United States SIGINT System (USSS) to collect and disseminate communications of or concerning that person for foreign intelligence purposes, to include but not limited to force protection, hostage recovery, and other like purposes.

H1.2. (U//~~FOUO~~) Forms 1 and 2 can be used to obtain and record consent to collect and disseminate a U.S. person's communications as well as references to the U.S. person in communications. Forms 3 and 4 only provide consent to collect and disseminate references to the U.S. person but neither Form 3 nor Form 4 provides consent to collect communications to or from the U.S. person who has executed the form. Each form contained in this Annex may be reproduced, provided the security classifications (top and bottom) are removed. It is the responsibility of the user to properly reclassify the consent form that is suitable to the user's purposes in accordance with requisite security guidelines and operational considerations of the customer whom the USSS is supporting.

H1.3. (U) Section 4.1.c. of United States Signals Intelligence Directive SP0018 states that the Director of NSA (DIRNSA) has authority to approve the consensual collection of communications to, from, or about U.S. persons. Elements of the USSS proposing to conduct consensual collection should forward a copy of the executed consent form and any pertinent information to the DIRNSA (or to the Senior Operations Officer of the National Security Operations Center) for approval of the proposed consensual collection activity. NSA OGC must also be notified promptly of the proposed collection activity.

H1.4. (U) If operational circumstances dictate, consent may be obtained orally or may be recorded on a form other than one of the forms contained in this Annex. However, any other form or method that is used to obtain and record a U.S. person's consent for elements of the USSS to collect and disseminate communications of or concerning that person must be reviewed and approved by NSA OGC.

CONSENT FORM 1

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

NSA SIGNALS INTELLIGENCE CONSENT AGREEMENT

I, _____, hereby consent to the National Security Agency or other elements of the United States Signals Intelligence System undertaking to seek and disseminate communications to, from, or referencing me for the purpose of _____

I understand that, unless specified otherwise in the purpose above, communications to, from, or referencing me may be sought and disseminated while I am in the U.S. during the effective period of my consent. This consent applies to administrative messages alerting elements of the United States Signals Intelligence System to this consent, as well as to any signals intelligence reports that may relate to the purpose stated above.

Except as otherwise provided by law, to include procedures under Executive Order 12333, this consent covers only information that relates to the purpose stated above and is effective for the period:

_____ to _____

Signals intelligence reports containing information derived from communications to, from, or referencing me may only be disseminated to me and to _____ and to others as specified by the U.S. Government as otherwise permitted by law, to include procedures under Executive Order 12333.

Signature

Date

Title

PRIVACY ACT STATEMENT: Authority for collecting information is contained in Section 6 of the National Security Agency Act of 1959, Public Law 86-36, codified at 50 U.S.C. 402 note; Executive Order (E.O.) 12333, as amended; and E.O. 13526. NSA's Blanket Routine Uses found at 58 Fed. Reg. 10,531 (1993) and the specific uses found in GNSA 18 apply to this information. Disclosure of requested information is voluntary but refusal to provide requested information may prevent NSA from effecting this consent form.

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET - SI - REL TO USA, FVEY~~

CONSENT FORM 2

CONSENT AGREEMENT

I, _____, hereby consent to the U.S. Government undertaking to seek and disseminate communications to, from, or referencing me for the purpose of:

I understand that, unless specified otherwise in the purpose above, communications to, from, or referencing me may be sought and disseminated while I am in the U.S. during the effective period of my consent. This consent applies to administrative messages alerting elements of the U.S. Government to this consent, as well as to any reports that may relate to the purpose stated above.

Except as otherwise provided by law, to include applicable U.S. Government procedures, this consent covers only information that relates to the purpose stated above and is effective for the period:

_____ to _____

Reports containing information derived from communications to, from, or referencing me may only be disseminated to me and to _____, and to others as specified by the U.S. government as otherwise permitted by law, to include applicable U.S. Government procedures.

Signature

Date

Title

PRIVACY ACT STATEMENT: Authority for collecting information is contained in Executive Order 12333, as amended; and procedures issued thereto. The Department of Defense Blanket Routine Uses found at:

http://privacy.defense.gov/blank_et_uses.shtml

apply to this information. Disclosure of requested information is voluntary but refusal to provide requested information may prevent completion of actions to effect this consent form.

~~SECRET - SI - REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

CONSENT FORM 3

NSA SIGNALS INTELLIGENCE CONSENT AGREEMENT

I, _____, hereby consent to the National Security Agency or other elements of the United States Signals Intelligence System undertaking to seek and disseminate communications referencing me for the purpose of:

I understand that, unless specified otherwise in the purpose above, communications referencing me may be sought and disseminated while I am in the U.S. during the effective period of my consent. This consent applies to administrative messages alerting elements of the United States Signals Intelligence System to this consent, as well as to any signals intelligence reports that may relate to the purpose stated above.

Except as otherwise provided by law, to include procedures under Executive Order 12333, this consent covers only references to me in foreign communications and information therefrom that relates to the purpose stated above and is effective for the period:

_____ to _____

Signals intelligence reports containing information derived from foreign communications referencing me may only be disseminated to me and to _____, and to others as specified by the U.S. Government as otherwise permitted by law, to include procedures under Executive Order 12333.

Signature

Date

Title

PRIVACY ACT STATEMENT: Authority for collecting information is contained in Section 6 of the National

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA FVEY~~

Security Agency Act of 1959, Public Law 86-36, codified at 50 U.S.C. 402 note; Executive Order (E.O.) 12333, as amended; and E.O. 13526, NSA's Blanket Routine Uses found at 58 Fed. Reg. 10,531 (1993) and the specific uses found in GNIA 18 apply to this information. Disclosure of requested information is voluntary but refusal to provide requested information may prevent NSA from effecting this consent form.

CONSENT FORM 4

CONSENT AGREEMENT

I, _____, hereby consent to the U.S. Government undertaking to seek and disseminate communications referencing me for the purpose of:

I understand that, unless specified otherwise in the purpose above, communications referencing me may be sought and disseminated while I am in the U.S. during the effective period of my consent. This consent applies to administrative messages alerting elements of the U.S. Government to this consent, as well as to any reports that may relate to the purpose stated above.

Except as otherwise provided by law, to include applicable U.S. Government procedures, this consent covers only references to me in foreign communications and information therefrom that relates to the purpose stated above and is effective for the period:

_____ to _____

Reports containing information derived from foreign communications referencing me may only be disseminated to me and to _____, and to others as specified by the U.S. government, as otherwise permitted by law, to include applicable U.S. Government procedures.

Signature

Date

Title

PRIVACY ACT STATEMENT: Authority for collecting information is contained in Executive Order 12333, as

~~SECRET//SI//REL TO USA FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

amended, and procedures issued thereto. The Department of Defense Blanket Routine Uses found at http://privacy.defense.gov/blank_et_uses.shtml

apply to this information. Disclosure of requested information is voluntary but refusal to provide requested information may prevent completion of actions to effect this consent form.

USSID SP0018

ANNEX I - (U) FORM FOR CERTIFICATION OF OPENLY ACKNOWLEDGED ENTITIES

SECTION 1 - CERTIFICATION FORM

(U) Certification Form

11.1. (U) The form below should be used for Director approvals for the collection of communications of entities that are openly acknowledged to be directed and controlled by a foreign power as specified in Section 4 of this USSID.

DIRECTOR, NSA/CHIEF, CSS

Certification for Openly Acknowledged Entities Under Section 4.A.1.(b) of the Classified Annex to DOD 5240.1R

Certification to the Attorney General:

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(S//SI//REL)~~ The Director, NSA, hereby certifies that [redacted] located in the United States and openly acknowledged to be directed and controlled by (Government X), is a new target of collection. The purpose of the surveillance is (to collect [redacted] intelligence regarding Government X) in accordance with valid intelligence requirements. The surveillance will entail intentional interception or deliberate selection of the target's international communications. Standard minimization procedures will be applied to any information collected that relates to U.S. persons.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

Director, NSA/Chief, CSS

Copy to: Deputy Secretary of Defense

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

USSID SP0018

ANNEX K - (S//REL)

[Redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

(b)(3)-P.L. 86-36

SECTION 1 - (U)

[Redacted]

(U)

K1 L (U)

[Redacted]

[Redacted]

[Redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

(S//SI//REL)

[Redacted]

[Redacted]

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086222

~~SECRET//SI//REL TO USA, FVEY~~

Proceed To:

NSA | Director | SIGINT | SIGINT Staff | SIGINT Policy Staff | USSID Index

Derived From: NSA/CSSM 1-52

Dated: 8 January 2007

Declassify On: 20360125

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086223

~~SECRET//SI//REL TO USA, FVEY~~



**UNITED
STATES
SIGNALS
INTELLIGENCE
DIRECTIVE**

USSID SP0018J
(formerly USSID 18J)

**(U//~~FOUO~~) PROCEDURES FOR MONITORING RADIO
COMMUNICATIONS OF SUSPECTED
INTERNATIONAL NARCOTICS TRAFFICKERS**

**OPC: The Signals Intelligence Directorate's Office of
Oversight and Compliance**

24 April 1986

LETTER OF PROMULGATION

~~(S//SI)~~ This Annex implements Section 2.3. and Section 2.6.(b) of Executive Order 12333, Section 372 and Section 374 of Title 10, United States Code, and special Attorney General procedures. It regulates certain COMINT activities of the United States Signals Intelligence System which are directed against radio communications of suspected international narcotics traffickers. SIGINT activities directed against international narcotics traffickers or trafficking activities that are not within the purview of this Annex are regulated by the basic USSID.

Approved for release by the
National Security Agency on
13 November 2013, FOIA
Case #71241

Derived From: NSA/CSSM 1-52

Dated

Declassify On

~~SECRET//SI//REL TO USA, FVEY~~

EXHIBIT
tabbles
AEX 17

DOCID: 4086223

~~SECRET//SI//REL TO USA, FVEY~~

(U//~~FOUO~~) This is the initial issue of this USSID SP0018, Annex J (formerly USSID 18, Annex J).

(U//~~FOUO~~) This USSID contains sensitive information that is legally protected from release to any member of the public and is to be used only for official purposes of the National Security Agency and its customers. Users must strictly adhere to all classification and handling restrictions (see (see NSA/CSS Classification Manual 123-2)) when storing hard or soft copies of this USSID or when hyperlinking to this USSID. The SIGINT Policy System Manager will maintain and update this USSID on-line where users may access the most current version from the NSANet. Appropriate USSIDs will also be available on INTELINK, as warranted. Users are responsible for the update and management of this USSID when it is stored locally.

(U//~~FOUO~~) United States SIGINT System (USSS) contractors or consultants assigned to NSA/CSS Headquarters or to other elements of the SIGINT Extended Enterprise are pre-authorized for access to USSIDs via NSANet, INTELINK, or in hard-copy formats as needed to perform their jobs. However, for those sensitive USSIDs for which access is password-controlled, all users, to include contractors, must undergo additional security and mission vetting. Non-USSS contractors or consultants working at external facilities are pre-authorized for soft-copy access to USSIDs via NSANet or INTELINK, if connectivity to those systems is allowed by the contractor's NSA/CSS sponsor. Where such connectivity is not established, any hard-copy provision of USSIDs must be authorized by the SIGINT Policy System Manager (NSTS: 963-3593, STU-III: (443) 479-1442, DSN: 644-7492).

(U//~~FOUO~~) This USSID is not releasable to any Third Party partner. If a shareable version of this USSID is needed (see USSID SP0002, Annex B (formerly USSID 2, Annex B)), please contact the appropriate Country Desk Officer in the Foreign Affairs Directorate.

THE EXECUTIVE AGENT:

/s/
WILLIAM E. ODOM
Lieutenant General, USA
Director, NSA/Chief, CSS

TABLE OF CONTENTS

SECTION 1 - (U) PURPOSE AND SCOPE

SECTION 2 - (U) DEFINITIONS

~~SECRET//SI//REL TO USA, FVEY~~

~~SECRET//SI//REL TO USA, FVEY~~

SECTION 3 - (U) COLLECTION

SECTION 4 - (U) RETENTION

SECTION 5 - (U) DISSEMINATION

SECTION 6 - (U) IDENTIFICATION OF U.S. PERSONS

SECTION 1 - (U) PURPOSE AND SCOPE

1.1. ~~(S//SI)~~ This Annex implements Section 2.3., and Section 2.6.(b) of Executive Order 12333, Section 372, and Section 374 of Title 10, United States Code, and special Attorney General procedures. It regulates certain COMINT activities of the **United States SIGINT System (USSS)** which are directed against radio communications of suspected international narcotics traffickers. Nothing contained in this Annex affects the basic authority of the USSS to collect and disseminate foreign intelligence regarding aspects of international narcotics trafficking activities, including [redacted] other than those activities expressly addressed herein. SIGINT activities directed against international narcotics traffickers or trafficking activities that are not within the purview of this Annex are regulated by the basic USSID.

1.2. (U//~~FOUO~~) The provisions of this Annex will be implemented only upon specific instruction from DIRNSA/CHSS or his designee.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

SECTION 2 - (U) DEFINITIONS

2.1. ~~(S//SI)~~ The following definitions apply to this Annex only. Unless contradicted or otherwise supplemented by these definitions, the definitions contained in Section 3 of the basic USSID SP0018 (formerly USSID 18) also apply to this Annex.

a. ~~(S//SI)~~ **International Narcotics Trafficker:** Any person engaged in buying, selling, manufacturing (to include any step in the process from cultivation to refining), or transporting controlled substances, as defined by the Attorney General, where such activities cross international boundaries.

b. ~~(S//SI)~~ [redacted]

c. ~~(S//SI)~~ [redacted]

~~SECRET//SI//REL TO USA, FVEY~~

~~SECRET//SI//REL TO USA, FVEY~~

[Redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

d. ~~(S//SI)~~ **Wire Communications:** Any communication carried in whole or part by wire, cable or other like connection furnished or operated by any person engaged as a common carrier in providing or operating such facilities for the transmission of interstate or foreign communications. Wire communications enjoy a reasonable expectation of privacy. The USSS may intentionally intercept communications of a U.S. person under circumstances where there is a reasonable expectation of privacy of such communications, only with prior authorization of the Attorney General, an order of the Foreign Intelligence Surveillance Court, or prior consent of the U.S. person. Thus, [Redacted]

[Redacted] under this Annex.

e. ~~(S//SI)~~ **United States:** When used in a geographic sense, the term, "United States," means all areas under the territorial sovereignty of the United States.

f. ~~(S//SI)~~ **Territorial Limits:** The waters and airspace adjacent to the United States, its territories and possessions, to a distance of twelve miles from the coastline. A communicant whose location has not otherwise been determined will be deemed a communicant outside the territorial limits unless the nature of the communications or other elements in the content or circumstances of the communications give rise to a reasonable belief that the communicant is located inside the territorial limits of the United States.

SECTION 3 - (U) COLLECTION

3.1. ~~(S//SI)~~ The USSS is authorized to intercept and to perform direction finding against the radio communications of persons, including U.S. persons, whom the USSS reasonably suspects to be engaged in international narcotics trafficking activities when:

a. ~~(S//SI)~~ All communicants are located outside the United States and its territorial limits and either:

(1) ~~(S//SI)~~ There exists a reasonable basis for belief that not all communicants are U.S. persons; or,

(2) ~~(S//SI)~~ At least one of the communicants is [Redacted] and the communications are expected to contain information concerning [Redacted] illicit narcotics.

b. ~~(S//SI)~~ All communicants are located inside the United States and its territorial limits and:

(1) ~~(S//SI)~~ At least one of the communicants is [Redacted] which is [Redacted] (b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

~~SECRET//SI//REL TO USA, FVEY~~

~~SECRET//SI//REL TO USA, FVEY~~

(2) (S//SI) The communicants are reasonably suspected to be engaged in narcotics trafficking activities at the time of interception; and,

(3) (S//SI) Collection is solely for the purpose of acquiring information related to [redacted] illicit narcotics shipments.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

c. (S//SI) Some communicants are located inside, and others located outside, the United States and either:

(1) (S//SI) The communicant to be targeted is located outside the territorial limits; or,

(2) (S//SI) The communicant to be targeted is located [redacted] within the territorial limits, but beyond the coastline of the United States.

3.2. (C) [redacted]

3.3. (C) Collection authorized under sub-paragraph 3.1.a. and subparagraph 3.1.c. (but not that authorized under sub-paragraph 3.1.b.) may be performed in support of the NSA foreign intelligence mission in response to foreign intelligence requirements approved by the Director of Central Intelligence.

SECTION 4 - (U) RETENTION

4.1. (S//SI) Information obtained in the course of the collection authorized under paragraph 3.1. that identifies U.S. persons, or communications obtained in the course of collection authorized under sub-paragraph 3.1.b. and subparagraph 3.1.c., that are solely between U.S. persons, may be retained no longer than one year from the date of intercept unless:

a. (S//SI) The SIGINT Director approves a longer retention period to support technical data bases;

b. (S//SI) The information is disseminated in accordance with Section 5, in which case retention is authorized for whatever period is deemed necessary to satisfy analytic requirements;

c. (S//SI) The communications from which the information is derived are encrypted, or are reasonably believed to contain a secret meaning, in which case retention for an indefinite period is authorized; or,

d. (S//SI) [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

~~SECRET//SI//REL TO USA, FVEY~~

~~SECRET//SI//REL TO USA, FVEY~~

4.2. (S//SI) Communications solely between U.S. persons acquired under subparagraph 3.1.a. (but not under subparagraph 3.1.b. and subparagraph 3.1.c.), shall be disposed of upon recognition, except that:

a. (S//SI) Technical data concerning frequency and channel use (example: callsigns, broadcast schedules, signal characteristics, etc.) may be retained for collection avoidance purposes; and,

b. (S//SI) Information concerning [redacted] illicit narcotics shipments may be retained in accordance with paragraph 4.1., when at least one communicant is [redacted]

[redacted]

SECTION 5 - (U) DISSEMINATION

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

5.1. (S//SI) Dissemination of information of, or concerning, U.S. persons, derived from collection under subparagraph 3.1.a., is governed by Section 8 of the basic USSID, except that:

a. (S//SI) Information concerning [redacted] illicit narcotics shipments may be disseminated to appropriate federal law enforcement agencies when:

(1) (S//SI) Not all communicants are U.S. persons; or,

(2) (S//SI) All communicants are U.S. persons, and at least one communicant is

[redacted]

b. (S//SI) Technical data concerning frequency and channel use may be disseminated to appropriate federal law enforcement agencies regardless of whether the communicants are U.S. persons or not.

5.2. (S//SI) Dissemination of information derived from collection under subparagraph 3.1.b. may be made only to appropriate federal law enforcement agencies, and only when the information relates to [redacted] illicit narcotics shipments. Technical data concerning frequency and channel use may be disseminated to appropriate law enforcement agencies even when the underlying communications do not contain information on [redacted] illicit narcotics shipments.

5.3. (S//SI) Dissemination of information concerning U.S. persons, derived from collection performed under subparagraph 3.1.c., may be made when:

a. (S//SI) The information is derived from monitoring communicants located outside the U.S. territorial limits:

(1) (S//SI) To appropriate federal law enforcement agencies when the information concerns [redacted] illicit narcotics shipments; or,

(2) (S//SI) In accordance with Section 8 of the basic USSID, when there exists a reasonable belief that not all communicants are U.S. persons.

b. (S//SI) The information is derived from monitoring communicants located inside U.S. territorial limits:

~~SECRET//SI//REL TO USA, FVEY~~

~~SECRET//SI//REL TO USA, FVEY~~

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)
(b)(3)-18 USC 798

(1) ~~(S//SI)~~ Only to appropriate federal law enforcement agencies; and

(2) ~~(S//SI)~~ Only insofar as the information relates to illicit narcotics shipments.

c. ~~(S//SI)~~ Technical data concerning frequency and channel use, and direction finding results, derived from any communication monitored under subparagraph 3.1.c. may be disseminated to appropriate law enforcement agencies.

5.4. ~~(U//FOUO)~~ Information collected under subparagraph 3.1.a and subparagraph 3.1.c. may be disseminated to appropriate federal authorities when no information of, concerning, U.S. persons is involved.

5.5. ~~(S//SI)~~ Access to technical data bases will be restricted to SIGINT collection and analytic personnel. Requests for access from other personnel or entities shall be referred to the SIGINT Director, except that technical data concerning frequency and channel use, and direction finding results, derived from collection performed under Section 3, may be disseminated to appropriate federal law enforcement agencies without specific SIGINT Director approval.

5.6. ~~(C//SI)~~ Information revealing a threat to human life or physical safety may be disseminated by field elements to appropriate federal authorities without prior review by the SIGINT Director. On the other hand, dissemination of such information by NSA Headquarters' elements requires prior approval of the SIGINT Director. The **National Security Operations Center (NSOC), Senior Operations Officer (SOO)**, is authorized to approve dissemination after normal duty hours or in time-sensitive situations.

5.7. ~~(C//SI)~~ Information derived from intercepted communications, solely between U.S. persons, which does not relate to illicit narcotics, but which reveals significant foreign intelligence or counterintelligence affecting substantial national security interests, may be disseminated to appropriate federal authorities, if approved by DIRNSA.

SECTION 6 - (U) IDENTIFICATION OF U.S. PERSONS

6.1. ~~(C)~~ Field elements may provide the identities of U.S. persons to federal authorities when the information relates to a threat to human life or physical safety without prior case-by-case approval of the SIGINT Director.

6.2. ~~(C//SI)~~ In all other cases, identification of U.S. persons in information disseminated outside the SIGINT system requires approval of the SIGINT Director. After normal duty hours or in time-sensitive situations the NSOC SOO is authorized to act for the SIGINT Director.

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4086223

~~SECRET//SI//REL TO USA, FVEY~~

Proceed To:

NSA | Director | SIGINT | SIGINT Staff | SIGINT Policy | USSID Index

Derived From: NSA/CSS Manual 123-2

Dated: 24 Feb 1998

Declassify On: 20291123

~~SECRET//SI//REL TO USA, FVEY~~

DOCID: 4145833

~~SECRET//COMINT//REL TO USA, FVEY~~



SIGNALS INTELLIGENCE
DIRECTORATE

SID MANAGEMENT DIRECTIVE NUMBER
432

Issue Date: 5 May 2010

Revised Date:

POC: SID Policy Staff, S0231

~~(C//REL)~~ PROCEDURAL GUIDELINES FOR
SIGINT PRODUCTION ON
U.S. [REDACTED] FIELD EXERCISES

(U) Purpose
(Heading 5,
Block Label))

~~(S//REL)~~ These guidelines apply to collection and dissemination of SIGINT
on the activity of [REDACTED]

The purpose is to enable elements of the SIGINT production chain to:

- Understand the distinctive set of responsibilities for these events,
- Execute preparatory procedures in the right timeframe,
- Ensure compliance with law and policy,
- Optimize reporting,
- Disseminate product appropriately, and
- [REDACTED]

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-18 USC 798
(b) (3)-50 USC 3024 (i)

~~SECRET//COMINT//REL TO USA, FVEY~~



DOCID: 4145833

~~SECRET//COMINT//REL TO USA, FVEY~~

(U) Scope These guidelines pull together pertinent provisions from several separate U.S. SIGINT Directives (USSIDs), policies, and directives, and define procedural steps for their practical application in a timely fashion.

(U//~~FOUO~~) **Cautionary Note:** These guidelines pertain to actual SIGINT production responding to real Information Needs (INs) in the National SIGINT Requirements Process (NSRP). These guidelines do not pertain to "Exercise SIGINT" which is simulated, serves the artificial exercise scenario, and has no validity as intelligence (see USSIDs SP0018, ANNEX C, and CR1221).

//s//

WILLIAM M. CRUMM
Signals Intelligence Director

DISTRIBUTION:
Signals Intelligence Directorate (all organizations)
SIGINT Enterprise, Field, (all organizations)

~~SECRET//COMINT//REL TO USA, FVEY~~

~~SECRET//COMINT//REL TO USA, FVEY~~

(U) BACKGROUND

(U) Background

1. ~~(S//SI//REL)~~ U.S. [redacted] exercises provide windows of opportunity for unique SIGINT production. Exercise related communications [redacted]

(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 18 USC 798
(b) (3) - 50 USC 3024 (i)

2. ~~(S//SI//REL)~~ [redacted]

(U) POLICY

(U) Policy Summary

3. (U//~~FOUO~~) This policy is intended to facilitate early anticipation and enable informed execution of each special preparatory step for SIGINT collection for this type of exercise scenario. This guidance is intended for any U.S. SIGINT System (USSS) element involved -- including Cryptologic representatives at U.S. Combatant Commands (COCOMs), Second Party liaison offices, and Target Offices of Primary Interest (TOPIs) -- to enable them to work in time and in concert to navigate procedural requirements.

~~SECRET//COMINT//REL TO USA, FVEY~~

~~SECRET//COMINT//REL TO USA, FVEY~~

**(U) Policy
Guidance and
Procedures**

4. (U) The following sections of relevant policy provide the primary guidance and procedures that apply for conditions covered under this guidance.

- (U) USSID SP0018, Annex H, specifies approval channels for consensual collection and dissemination of SIGINT on U.S. persons and provides "Consent Agreement" forms for SIGINT coverage that include specifications on dissemination of derived reporting.
- (U//~~FOUO~~) Both USSID SP0018, Section 7, and USSID CR1400, Section 3, address dissemination of the identities of U.S. persons.

• ~~(C//SI//REL)~~ [Redacted]

(b) (1)
 (b) (3) - P.L. 86-36
 (b) (3) - 18 USC 798
 (b) (3) - 50 USC 3024 (i)

- (U//~~FOUO~~) The Oversight and Compliance Manual "U.S. Identities in SIGINT (U)" provides additional guidance on dissemination of the identities of U.S. and Second Party persons in SIGINT.

(U) PROCEDURES

(U) Procedures

5. (U//~~FOUO~~) This section lays out procedural steps to accomplish USSID or policy requisites for collection and dissemination on a U.S. [Redacted] (b) (3) - P.L. 86-36 field exercise of interest, namely:

- documented customer requirements/needs,
- special authorizations for collection,
- reporting on U.S. persons [Redacted] and
- dissemination constraints.

**(U)
Information
Needs (IN)**

6. (U//~~FOUO~~) Ensuring a basis of Information Need(s): The unique intelligence gathering opportunity of a U.S. [Redacted] exercise is only SIGINT exploitable if there is an applicable IN(s) in the NSRP. Cryptologic Services Groups (CSGs) are positioned to both understand the particular exercise-related intelligence requirements of their

~~SECRET//COMINT//REL TO USA, FVEY~~

DOCID: 4145833

~~SECRET//COMINT//REL TO USA, FVEY~~

customers and to help customers articulate any new requirements in the NSRP as INs. Follow the steps below to submit a Limited Focus IN to cover the specific exercise. Be sure to take note of the timeline applicable.

- (U//~~FOUO~~) As soon as the dates are established for the exercise, the customer, assisted by the appropriate CSG should begin drafting a Limited Focus IN. The Limited Focus IN is meant to cover specific events and issues. Obtaining SIGINT on exercises may require development/relocation of collection assets, establishment/improvement of dataflow and processing, and/or manpower adjustments. It may not be possible to address INs submitted close to the exercise start date.
- (U//~~FOUO~~) Research within NSRP the existing INs which already address the area/entities of concern for the specified exercise. If assistance is required on how to create queries in NSRP, email DL nsrpteam@nsa.ic.gov. Reference related IN number(s) in the new Limited Focus IN.
- (U//~~FOUO~~) The customer must pay attention to the SIGINT priority assigned per their National Intelligence Priorities Framework table choices. If the SIGINT priority is low and the customer cannot justify an upward change of priority, the SIGINT system may not have the resources to support the exercise. It is the customer's responsibility to seek a higher priority.
- (U//~~FOUO~~) The customer then submits the IN for validation. Customers should plan that the validation process will typically require at least 3 weeks before the IN is levied upon NSA. (Note: INs can be submitted months before the scheduled event).
- (U//~~FOUO~~) The customer should request a Level of Effort (LOE) statement with a suspense date that is no sooner than 14 days from the date of Final National Validation for the IN. The LOE is intended to shape customer expectations and serve as a jumping off point for further discussion.
- (U//~~FOUO~~) As the actual dates of the exercise approach or changes to the customer need are recognized, a new version of the IN should be immediately created and submitted to reflect these changes and give the SIGINT system the greatest opportunity to adjust to meet the revised need.

(b) (3) - P.L. 86-36

(U) Collection

7. (U//~~FOUO~~) Collection - Step A. U.S. Consent Forms: The TOPI is~~SECRET//COMINT//REL TO USA, FVEY~~

~~SECRET//COMINT//REL TO USA, FVEY~~

responsible for determining whether it may be necessary to collect U.S. communications to get adequate SIGINT on the applicable INs during the [redacted] exercise of interest. Follow the steps below for consent forms to collect and disseminate on U.S. persons' communications during the exercise. Again, for successful planning, be sure to take note of the time required for each step.

8. (U//~~FOUO~~) Individuals giving consent to NSA to collect and disseminate foreign communications about their activities must submit a signed consent form (see USSID SP0018, ANNEX H). A justification, drafted by either the individual giving consent or the person requesting consensual collection of a U.S. person, must accompany the signed consent form and should address the following:

(b) (3) - P.L. 86-36

- identity of and sufficient information about the person(s) giving consent,
- mission-related purpose of the request,
- location of activity in which person(s) giving consent will be involved,
- time period for consensual collection,
- TOPI providing SIGINT support for the activity, and
- Organizations, agencies, individuals authorized to receive SIGINT reports related to consensual collection.

(b) (3) - P.L. 86-36

9. (U//~~FOUO~~) The signed consent form and the justification must be submitted via secure email to DL CONSENSUAL or secure fax [redacted] [redacted] SV drafts the documentation for coordination and approval. The process typically requires 30 days to complete. D/DIR is the final approval authority for consensual collection.

10. (C//~~REL~~) [redacted]

(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 18 USC 798
(b) (3) - 50 USC 3024(i)

11. (C//~~SI/REL~~) [redacted]

~~SECRET//COMINT//REL TO USA, FVEY~~

DOCID: 4145833

~~SECRET//COMINT//REL TO USA, FVEY~~

[Redacted]

12. ~~(C//SI//REL)~~

[Redacted]

[Redacted]

(b) (1)
 (b) (3) - P.L. 86-36
 (b) (3) - 18 USC 798
 (b) (3) - 50 USC 3024(i)

13. ~~(C//REL)~~

[Redacted]

[Redacted]

~~(C//REL)~~

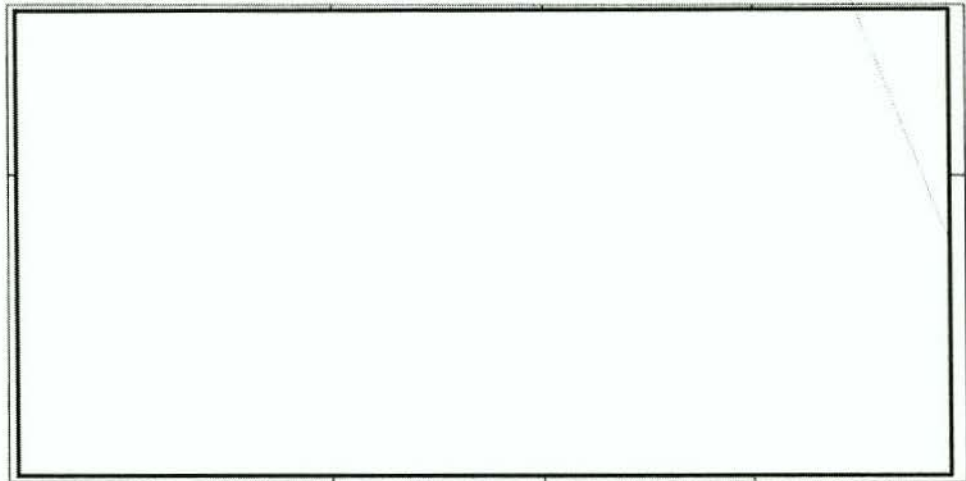
REQUEST PROCEDURES AND SCHEDULE FOR COLLECTION			
Action	60 days prior	30 days prior	At least 14 days prior
For collection on U.S. participants: TOPI submits email of signed consent forms and justifications to DL CONSENSUAL (Oversight and Compliance)		X	

~~SECRET//COMINT//REL TO USA, FVEY~~

DOCID: 4145833

(b) (1)
(b) (3)-P.L. 86-36
(b) (3)-18 USC 798
(b) (3)-50 USC 3024(i)

~~SECRET//COMINT//REL TO USA, FVEY~~



~~(C//REL)~~

(U) Analysis and Reporting

14. (U//~~FOUO~~) Analysis and Reporting: SIGINT policy on handling U.S. identities in SIGINT reporting can be found in:

- USSID SP0018, particularly sections 4 through 7;
- USSID CR1400, section 3 (which also addresses handling of Second Party identities); and
- "U.S. Identities in SIGINT" manual.

15. The Information Sharing Services organization provides a collection of useful reference information on this topic in "The USSID SP0018 Corner" which includes guidance on Second Party identities. These resources are applied and reinforced by knowledgeable SIGINT reporters in many entities across the SIGINT enterprise who, in their daily tasks, observe protective processes and procedures for references to U.S. persons in SIGINT report preparation. For issues in reporting on U.S. exercises, the first approach for resolution lies in direct utilization of these documentary and collegial resources.

(b) (3)-P.L. 86-36

~~SECRET//COMINT//REL TO USA, FVEY~~

DOCID: 4145833

~~SECRET//COMINT//REL TO USA, FVEY~~(U)
Dissemination

16. (U//~~FOUO~~) Dissemination: Consent forms for collection of U.S. persons' communications also include space for consent for dissemination to specifically listed entities. While there may be only one external customer responsible for requesting the special SIGINT effort on a U.S. [] exercise, SIGINT reporting policy does not permit limiting product dissemination to only one recipient. Once the consent form has been properly filled out, and a request for guidance has been submitted, Information Sharing Services, Pre-publication Services [] will, in conjunction with the appropriate TOPIs, provide exercise specific guidance for analysts and reporters. Unless otherwise limited, these reports will be addressed, at a minimum, to ODNI and DEPT of DEF, including the participating COCOM Commander(s). Any special handling instructions requested by either the participants or the TOPI(s) can be incorporated into the guidance, to insure consistency of coverage. The guidance will include at a minimum, the following information:

(b) (3) - P.L. 86-36

- Start and end dates of exercise
- Start and end dates of coverage (usually longer)
- Information on the type of exercise being conducted
- Terrorism/threat reporting guidance and distro instructions (if applicable)
- General reporting guidance and distro suggestions
- Pertinent INs
- Sensi-check guidance (if applicable)
- IPO caveat guidance (almost always, from now on)
- Terms of the consensual collection/dissemination agreement
- Points of Contact (TOPIs and RPG)

 (U) GLOSSARY

~~SECRET//COMINT//REL TO USA, FVEY~~

~~SECRET//COMINT//REL TO USA, FVEY~~

(U) Host
Nation

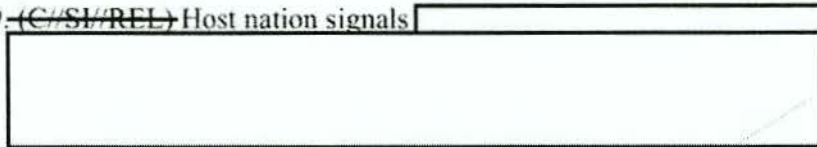
17. ~~(C//REL)~~ USSID SP0009, dated 22 February 2006 defines "Host Nation" as:

"The United Nations-recognized foreign nation on whose territory (including soil, territorial waters, or airspace) a U.S. SIGINT operation has been established, to which a temporary or permanent mobile USSS asset may be deployed, or in which a U.S. SIGINT activity is being conducted with the approval of that government. The specific U.S. SIGINT mission may be declared or undeclared officially to the host government. For mobile operations, "host nation" is defined as the foreign country in which a mobile SIGINT platform is either based or visiting either in a declared or undeclared status with the general knowledge and/or approval of that nation's government."

18. ~~(C//REL)~~ Within the SIGINT Community, the usage of the term "Host Nation" generally excludes Second Party countries, to which USSID SP0009 does not apply. Most Third Party SIGINT partner countries fall under the provisions of USSID SP0009.

(U) Host
Nation Signals

19. ~~(C//SI//REL)~~ Host nation signals



(b) (1)
(b) (3) - P.L. 86-36
(b) (3) - 18 USC 798
(b) (3) - 50 USC 3024 (i)

~~SECRET//COMINT//REL TO USA, FVEY~~