

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

FOIA Case: 84993B 4 March 2021

MR. RUSS KICK

Dear Russ Kick:

This responds to your Freedom of Information Act (FOIA) request of 15 July 2016 stating "The Federal Agency Data Mining Report Act requires any department or agency engaged in data mining to submit an annual updated report on this activity to Congress and to make the reports available to the public. I request the last two such reports created by the NSA." A copy of your request is enclosed. As previously provided, your request has been processed under the FOIA, and the documents you requested are enclosed. Certain information, however, has been withheld from the enclosures.

Some of the withheld information has been found to be currently and properly classified in accordance with Executive Order 13526. The 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 Executive Order 13526. 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 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); and Section 6, Public Law 86-36 (50 U.S. Code 3605).

Since these withholdings may be construed as a partial denial of your request, you are hereby advised of this Agency's appeal procedures.

You may appeal this decision. If you decide to appeal, you should do so in the manner outlined below. NSA will endeavor to respond within 20 working days of receiving any appeal, absent any unusual circumstances.

The appeal must be sent via U.S. postal mail, fax, or electronic delivery (e-mail) and addressed to:

FOIA Case: 84993B

NSA FOIA/PA Appeal Authority (P132) National Security Agency 9800 Savage Road STE 6932 Fort George G. Meade, MD 20755-6932

The facsimile number is 443-479-3612. The appropriate email address to submit an appeal is FOIARSC@nsa.gov.

- ξ It must be postmarked or delivered electronically no later than 90 calendar days from the date of this letter. Decisions appealed after 90 days will not be addressed.
- ξ Please include the case number provided above.
- ξ Please describe with sufficient detail why you believe the denial of requested information was unwarranted.

You may also contact our FOIA Public Liaison at foialo@nsa.gov for any further assistance and to discuss any aspect of your request. Additionally, you may contact the Office of Government Information Services (OGIS) at the National Archives and Records Administration to inquire about the FOIA mediation services they offer. The contact information for OGIS is as follows:

Office of Government Information Services National Archives and Records Administration 8601 Adelphi Rd. - OGIS College Park, MD 20740 ogis@nara.gov 877-684-6448 (Fax) 202-741-5769

> Sincerely, Sharn C Luki

RONALD MAPP Chief, FOIA/PA Office NSA Initial Denial Authority

Encls: a/s

-					
-	•	8	٧	٩	٠
	v	ı		5	

donotreply@nsa.gov

Sent:

Friday, July 15, 2016 9:02 AM

To:

donotreply@nsa.gov

Subject:

FOIA Request (Web form submission)

Title: Mr.

Full Name: Russ Kick

email:

Postal Address:

Postal City:

Postal State-prov:

Zip Code:

Country: United States of America

Home Phone:

Records Requested: The Federal Agency Data Mining Reporting Act requires any department or agency engaged in data mining to submit an annually updated report on this activity to Congress and to make the reports available to the public.

I request the last two such reports created by the NSA.

Further, I request that these files be sent to me in any digital formats in which they exist (PDF, Word, etc.). Under the terms of the E-FOIA Amendments of 1996, Section 5, if a document exists in electronic format, it must be released in that format upon request.

National Security Agency/Central Security Service

Federal Agency Data Mining Report for Fiscal Year (FY) 2017

Introduction.

The National Security Agency/Central Security Service (NSA) has prepared this report in response to Section 804, Public Law 110-53, Federal Agency Data Mining Reporting Act of 2007 (the Act), which requires "the head of each department agency of the Federal Government" to provide a report "not less frequently than annually...to include any activity to use or develop data mining," as defined by the Act. This report covers the data mining activities of all elements of NSA, has been produced in coordination with the Civil Liberties and Privacy Officer of NSA, and reflects a comprehensive review of NSA's data mining activities, as defined by the Act, for FY 17.

For the purposes of this report, "data mining" is defined as a NSA program involving patternbased queries, searches, or other analyses of one or more electronic databases where:

- (A) NSA is conducting the queries, searches, or other analyses to discover or locate a predictive pattern or anomaly indicative of terrorist or criminal activity on the part of any individual or individuals;
- (B) the queries, searches, or other analyses are not subject-based and do not use personal identifiers of a specific individual, or inputs associated with a specific individual or group of individuals, to retrieve information from the database or databases; and
 - (C) the purpose of the queries, searches, or other analyses is not solely:
 - (i) the detection of fraud, waste, or abuse in a Government agency or program; or
 - (ii) the security of a Government computer system.

This report does not include NSA queries, searches, or analyses of telephone directories, news reporting, free publicly-available information, or databases of judicial and administrative opinions or other legal research sources.

For details on NSA data mining activities, see the classified Annex included in this report.

Background.

Pursuant to its mission, NSA uses and develops communications data mining techniques for foreign intelligence purposes including detection of terrorist activity.

NSA is researching the use of commercial and academic data mining techniques to advance its authorized foreign intelligence mission through the science of discovery, which uses the patterns of a target group's activity to discover previously unknown members of the group. The goal is to identify previously unknown foreign terrorists, foreign intelligence officers, etc. within legally gathered foreign intelligence information.

TOT SECRET/SIMMOTORY

National Security Agency/Central Security Service

(U) Federal Agency Data Mining Report for Fiscal Year (FY) 2017 Classified Annex

(U) Introduction.

(U) The National Security Agency/Central Security Service (NSA) has prepared this Annex in compliance with Section (c)(3)(A) of Section 804, Public Law 110-53, Federal Agency Data Mining Reporting Act of 2007 (the Act), to address the classified data mining activities conducted at NSA during Fiscal Year (FY) 2017. This Annex will be made available to those entities required under Section (c)(3)(B) of the Act.

(U) Background.

- (U) Pursuant to its mission, NSA uses and develops communications data mining techniques for foreign intelligence purposes including detection of terrorist activity.
- (U) NSA researches the use of commercial and academic data mining techniques to advance its authorized foreign intelligence mission through the science of discovery. The goal is to use the patterns of a target group's activity to identify previously unknown foreign terrorists, foreign intelligence officers, etc. within legally gathered foreign intelligence information.

(U#FOUC) This report was completed by the NSA Civil Liberties and Privacy Office (CLPO), the Legislative State and Local Affairs Office, the Directorate of Operations, and the office of the General Counsel. The data mining activities in this 2017 report are the same activities that were in the previous year's report, and NSA's civil liberties and privacy assessment process is also unchanged. Therefore, there have been no substantive changes to NSA's assessments of these activities. As noted in last year's report, NSA's civil liberties and privacy assessment process describes the relevant facts using four categories of questions to assess the level of impact on individuals:

- How intrusive/comprehensive is the activity based on the data type(s)?
- How intentionally broad is the activity based on the scope of persons in the data?
- How unspecified/expansive is the activity based on the operational purpose and use of the data?
- How imprecise/inaccurate is the activity's methodology to achieve the operational purpose?

(U/TSUS) The assessments then describe the safeguards that NSA implements to mitigate and reduce these impacts.

(U/FOUC) NSA took steps to implement Presidential Policy Directive No. 28 (PPD-28) in FY 2014, such as revising its retention policy and factoring PPD-28 into its reviews of signals

Derived From: NSA/CSSM 1-52

Dated: 20130930

D. J. C. O. 20420701

TOP OPEN THE STATE OF STATE OF

intelligence programs. In January 2015, NSA adopted written supplemental procedures to formally implement PPD-28. Continuing its implementation, the assessments contained in this report assess impacts on all individuals, regardless of nationality, in keeping with PPD-28.

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

(U) NSA Classified Report for FY2017

	. 305		1
	NSA Classified Data Mining Activity #1 This table is classified FOP SECRECT//SI/MOPO		
	This table is classified TOP STONE TO THE TOP OF THE TO		
Title:	(U// FOUO)	:	
Title.	(0//1000)	<u> </u>	<u> </u>
		'	
Description:	(TS//SI/NT)		
		· ·	::•
7, 1			
		5	
		•	
		:	
		•	
		**	
36			
	(TS//SL//NT)	•:	: :
		•	 (
		.*	: :
		••	::
		•	
N		•:	: :
		••	
	7	::	: :
		·•	
		::	
		·•	
Technology	(TC//CL//DEL TO LICA EVEV)		
Used:			;
Oscu.			1 1 2
	* , 1		: 112
	l de la companya de		- : II :
		•	: 114
		•	. :
		•	1 1 1
Data Sources:	(TOHOUREL TO USA, EVEY)		- 2
	7 1		 :
Efficacy	(TOHOLIAT)		
Efficacy	(TOHOLITTIE)	The state of the s	
Assessment:			
			- 1
			- 1
			- 1

Doc ID: 6719287

TOP SECRET WILL MOTORN

(b) (1) (b) (3) -18 USC 798 (b) (3) -50 USC 3024(i)

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

Privacy Impact Assessment:	(U) Given that there are no changes to the activity, the 2016 assessment remains valid: (U) Using the civil liberties and privacy assessment process described in the Background section, this activity has the following impacts and employs the following safeguards: (U) This data mining activity is not intended to uncover patterns known to be engaged in by U.S. persons. (TS//SI//PEL TO USA, FVEY)
ii ii	(TS//SL//REL TO USA, FVEY) Purpose: The specified use of the analytic is to discover possible targets for a variety of foreign intelligence or counterintelligence missions. (TS//SL//REL TO USA, FVEY)

of signals intelligence.

Persons) and its Classified Annex. Furthermore, NSA's signals

intelligence activities must comply with the Fourth Amendment to the U.S. Constitution. The primary purpose of these requirements is to protect the rights and privacy of U.S. persons. The sum of these requirements is captured in NSA's Legal Compliance and Minimization Procedures,

USSID SP0018, which governs the collection, retention, and dissemination

¹ (U) Note that, effective 8 August 2016, the Secretary of Defense, in coordination with the Director of National Intelligence and with the approval of the Attorney General, issued DoD Manual 5240.01 to govern the conduct of DoD intelligence activities. DoDM 5240.01 supersedes Procedure 1-10 in DoD 5240.01-R. Procedures 11-15 of DoD 5240.01-R remain in effect. The Classified Annex remains in effect until updated or superseded.

Applicable Policies, Procedures, and Guidelines:

- (U) NSA incorporated the laws, regulations and guidelines listed above and other related procedures in an internal document, "Legal Compliance and U.S. Persons Minimization Procedures," also referred to as "U.S. Signals Intelligence Directive SP0018" or "USSID SP0018." These minimization procedures govern the entire process NSA follows when collecting, processing, retaining, and disseminating foreign intelligence that may contain U.S. person information. All NSA employees working with signals intelligence data are required to complete training to keep them abreast of legal requirements.
- (U) In addition to the laws, regulations, and guidelines that are implemented via USSID SP0018, the NSA adheres to Presidential Policy Directive No. 28, (PPD-28), which provides further policy direction for the United States' conduct of signals intelligence activities. Among other things, PPD-28 requires that the United States' signals intelligence activities "include appropriate safeguards for the personal information of all individuals... To the maximum extent feasible consistent with national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality."

TOP SECRET STATE ONLY

	NSA Classified Data Mining Activity #2 This table is classified TOP SECRET//SI//NOPORTY
Title:	(U/ /Peue)
Description:	(S//SI//REL TO USA, FVEY)
	(S//SI/REL TO USA, FVEY)
Technology Used:	(C//REL TO USA, FVEY)
	(C//CI//DEL TO LICA EVEX)
	(S//SL//REL TO USA, FVEY)
	(TC//CL//REL TO USA, FVEY)
	(Landinian To Con, TVLT)

,	
	CONTROL TO MALE PURE
,	
ū.	
	(S//SI/NT)
Data Sources:	(TC//SL/NIF)
	1 3 1
* **	
Efficacy	(TS//SI//REL TO USA, FVEY)
Assessment:	
	i ::: ::: ::: ::: ::: ::: ::: ::: ::: :
	1 11
Α	
	(C//SL/REL TO USA, FVEV)
-	H 1
	::
D' T	
Privacy Impact Assessment:	(U) Given that there are no changes to the activity, the 2016 assessment remains valid:
	(U) Using the civil liberties and privacy assessment process described in :
,	the Background section, this activity has the following impacts and employs the following safeguards:
	(U) This data mining activity is not intended to uncover patterns known to
	be engaged in by U.S. persons.
	(TC//SI/AIF)

(b) (1) (b) (3) -18 USC 798 (b) (3) -50 USC 3024(i)

(b)	131	-P.L.	86-36
121	101		00 50

	,	
		l .·` ÿ
		1 . 31
		(TS//SL/AIF)
		(15//52/112)
		· · · · · · · · · · · · · · · ·
		· ·
		(C//CL//REL TO USA, TVEY) Purpose: The purpose of this activity is to discover individuals who are potentially involved in terrorism human
		discover marviduas who are potentially involved in terrorism, naman
		trafficking, cyber attacks, and narcoterrorism
		The purpose and use for this activity is general foreign
		intelligence value
		1
		(TC//CI/ATT)
	27	
		(TC//CL/AIF)
		, v
(3)-P.I	L. 86-36	
	· · · · ·	(U//FOUC) Safeguards:
		NSA also

E WARREST ON THE PARTY HARRING THE WARRANT OF THE PARTY HARRING TH

procedures. Section 2.3 of E.O. 12333, as amended, specifies that elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning U.S. persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, after consultation with the Director of National Intelligence. NSA adheres to the limitations that are contained within those procedures and abides by the restrictions in its Attorney General-approved procedures specifically designed to provide protection to the privacy of U.S. persons. Pursuant to PPD-28, NSA implemented supplemental procedures extending comparable safeguards to all individuals, regardless of nationality. (TS//SL//PEL TO USA, FVEV) In order to further reduce the civil liberties and privacy impacts associated with this activity, key safeguards include: controlled access to users with completed training, documented justification for queries. auditing, dissemination restrictions to only that which is relevant for foreign intelligence or counterintelligence purposes, and retention limited to five years unless it has been specifically determined to be relevant for foreign intelligence or counterintelligence. The impact of this activity is also mitigated by the masking of U.S. and Second Party person results whenever they can be identified. (U) Section 1.7(c) of E.O. 12333 authorizes the Director, NSA to collect, Governing Laws and Regulations: process, analyze, produce, and disseminate signals intelligence for foreign intelligence and counterintelligence purposes to support national and departmental missions. The Secretary of Defense issued required procedures known as DoD Regulation 5240.1-R (Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons) and its Classified Annex.² Furthermore, NSA's signals intelligence activities must comply with the Fourth Amendment to the U.S. Constitution. The primary purpose of these requirements is to protect the rights and privacy of U.S. persons. The sum of these requirements is captured in NSA's Legal Compliance and Minimization Procedures, USSID SP0018, which governs the collection, retention, and dissemination of signals intelligence. Applicable (U) NSA incorporated the laws, regulations and guidelines listed above and Policies, other related procedures in an internal document, "Legal Compliance and Procedures, and U.S. Persons Minimization Procedures," also referred to as "U.S. Signals Guidelines: Intelligence Directive SP0018" or "USSID SP0018." These minimization procedures govern the entire process NSA follows when collecting, processing, retaining, and disseminating foreign intelligence that may contain U.S. person information. All NSA employees working with signals

² (U) See footnote 1.

TOP SECRET SUPPORTED

intelligence data are required to complete training to keep them abreast of legal requirements.

(U) In addition to the laws, regulations, and guidelines that are implemented via USSID SP0018, the NSA adheres to Presidential Policy Directive No. 28 (PPD-28), which provides further policy direction for the United States' conduct of signals intelligence activities. Among other things, PPD-28 requires that the United States' signals intelligence activities "include appropriate safeguards for the personal information of all individuals... To the maximum extent feasible consistent with national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality."

Doc ID: 6719287

T	NSA Classified Data Mining Activity #3 his table is classified TOT SECRET//SI//REL TO USA, TVEY	
Title:	(TS//SI//REL TO USA, TVEY)	4
	1	
	(C//CL//DEL TO LICA EVEV)	
Description:	(C//CL//DEL TO UCA, FVEY)	1
	3	
	1 3	
	(CUCUMPT TO LICA PUPLY)	7
		-4
	1	
	1 3	"
	1	- 1
Technology	(S//SI//REL TO USA, FVEY)	一
Used:		
	(CHCH/DEL TO LICA EVEV)	
	(G//GL//REL TO USA, FVEV)	\dashv
	1	
	·	ᅱ
	(S//SI//REL TO US/1. FVEY)	

TOT SECRET/ON MOTORIA

	・ 教 ・ 教 ・ 教 ・ 教 ・ 教 ・ 教 ・ 教 ・ 教 ・ 教 ・ 教
Data Sources:	(TO//CL//REL TO USA, FVLT)
	25 · 25 · 25 · 25 · 25 · 25 · 25 · 25 ·
Efficacy	(TS//SL/REL TO USA, FVEY)
Assessment:	# # # # # # # # # # # # # # # # # # #
Privacy Impact	(U) Given that there are no changes to the activity, the 2016 assessment.
Assessment:	remains valid: (U) Using the civil liberties and privacy assessment process described in the Background section, this activity has the following impacts and employs the following safeguards: (U) This data mining activity is not intended to uncover patterns known to be engaged in by U.S. persons. (TS//SL//DEL TO USA, FVET)
,	(TS//SL//DEL TO USA, FVEY)
	(TS//SI//REL TO USA, FYEY) Purpose: The purpose and use of these analytics is broadly defined to include any patterns to discover possible targets for any foreign intelligence or counterintelligence mission. As noted below, the purpose and uses are controlled through documented

Doc ID: 6719287	(b) (1) (b) (3) -18 USC 798
(b) (3)-P.L. 86-36	(b) (3) -50 USC 3024(i)
	(b) (3)-P.L. 86-36
	foreign intelligence/counterintelligence justifications for queries and auditing. (TS//SI//REL TO USA, TVET)
	(FS//SI/REL TO USA, FVET)
	(U//FOUS) Safeguards:
	protects the privacy rights of U.S. persons through its minimization procedures. Section 2.3 of E.O. 12333, as amended, specifies that elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning U.S. persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, after consultation with the Director of National Intelligence. NSA adheres to the limitations that are contained within those procedures and abides by the restrictions in its Attorney General-approved procedures specifically designed to provide protection to the privacy of
	U.S. persons. Pursuant to PPD-28, NSA implemented supplemental procedures extending comparable safeguards to all individuals, regardless of nationality. (TS://SI//REL TO USA, FVEY) In order to further reduce the civil liberties and privacy impacts associated with this activity, key safeguards include:

controlled access to users with completed training, documented justification for queries, auditing, dissemination restrictions to only

that which is relevant for foreign intelligence or counterintelligence

purposes, and retention limited to five years unless it has been specifically determined to be relevant for foreign intelligence or counterintelligence. Governing Laws (U) Section 1.7(c) of E.O. 12333 authorizes the Director, NSA to collect. and Regulations: process, analyze, produce, and disseminate signals intelligence for foreign intelligence and counterintelligence purposes to support national and departmental missions. The Secretary of Defense issued required procedures known as DoD Regulation 5240.1-R (Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons) and its Classified Annex.3 Furthermore, NSA's signals intelligence activities must comply with the Fourth Amendment to the U.S. Constitution. The primary purpose of these requirements is to protect the rights and privacy of U.S. persons. The sum of these requirements is captured in NSA's Legal Compliance and Minimization Procedures. USSID SP0018, which governs the collection, retention, and dissemination of signals intelligence. Applicable (U) NSA incorporated the laws, regulations and guidelines listed above and other related procedures in an internal document, "Legal Compliance and Policies, Procedures, and U.S. Persons Minimization Procedures," also referred to as "U.S. Signals Guidelines: Intelligence Directive SP0018" or "USSID SP0018." These minimization procedures govern the entire process NSA follows when collecting, processing, retaining, and disseminating foreign intelligence that may contain U.S. person information. All NSA employees working with signals intelligence data are required to complete training to keep them abreast of legal requirements. (U) In addition to the laws, regulations, and guidelines that are implemented via USSID SP0018, the NSA adheres to Presidential Policy Directive No. 28 (PPD-28), which provides further policy direction for the United States' conduct of signals intelligence activities. Among other things, PPD-28 requires that the United States' signals intelligence activities "include appropriate safeguards for the personal information of all individuals... To the maximum extent feasible consistent with national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality."

³ (U) See footnote 1.

Doc ID: 6719287

TOT SECRETIFICATION

Title: (TS//SI//REL TO USA, FVEY) Description: (S//SI//REL TO USA, FVEY)	
Description: (S//SI//REL TO USA, PVEY)	1
(S//SI//REL TO USA, FVEY)	
Technology Used:	

(b) (1)

	(TC//CL//DEL TO USA FATE)
	(TONISHINGE TO CSIL, I VEI)
D : 1	
Privacy Impact Assessment:	(U) Given that there are no changes to the activity, the 2016 assessment remains valid:
	(U) Using the civil liberties and privacy assessment process described in
	the Background section, this activity has the following impacts and employs the following safeguards:
	(U) This data mining activity is not intended to uncover patterns known to be engaged in by U.S. persons.
	(TS//SI//REL TO USA, FVEY)
	(TC//CI/AIF)
	(TS//SI//REL TO USA, FVEY) Purpose: The use of this activity is to track targets and discover new targets in support of a variety of foreign.
	intelligence and counterintelligence needs.
	(TS//SI//REL TO USA, FVEW)
	1 x 1 x
	(TC//CI//DEL TO LICA EVEV)

TOTAL SIDE OF THE PROPERTY OF THE PARTY OF T

1		was and the control of the control o
1 ⁰		
	- "	
	- 1	(U//FOCO) Safeguards:
		(OHT OCO) Sureguirds.
		NIC A
		also protects the privacy rights of U.S. persons through its minimization
		procedures. Section 2.3 of E.O. 12333, as amended, specifies that
(b) (3) -P	.L. 86-36	elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning U.S. persons only in accordance
	·	with procedures established by the head of the agency concerned and
	•••	approved by the Attorney General, after consultation with the Director of
	•	National Intelligence. NSA adheres to the limitations that are contained *within those procedures and abides by the restrictions in its Attorney
		General-approved procedures specifically designed to provide protection
		to the privacy of U.S. persons. Pursuant to PPD-28, NSA implemented supplemental procedures extending comparable safeguards to all
		individuals, regardless of nationality.
		(TS//SI//REL TO USA, FVEY) In order to further reduce the civil
		liberties and privacy impacts associated with this activity, key safeguards
		include: controlled access to users with completed training, documented
		justification for queries auditing, dissemination restrictions to only that which is relevant for foreign intelligence or counterintelligence
		purposes, and retention limited to five years unless it has been specifically
		determined to be relevant for foreign intelligence or counterintelligence. In addition, all queries conducted by analysts under this activity are
	-	subject to auditing and review to validate both the appropriateness of the
	Gaverning Lave	query conduced and the foreign intelligence or counterintelligence need.
	Governing Laws and Regulations:	(U) Section 1.7(c) of E.O. 12333 authorizes the Director, NSA to collect, process, analyze, produce, and disseminate signals intelligence for foreign
		intelligence and counterintelligence purposes to support national and
	-	departmental missions. The Secretary of Defense issued required procedures known as DoD Regulation 5240.1-R (Procedures Governing
		the Activities of DoD Intelligence Components That Affect United States
		Persons) and its Classified Annex. ⁴ Furthermore, NSA's signals intelligence activities must comply with the Fourth Amendment to the
		U.S. Constitution, and must be conducted in accordance with FISA and
		FAA. The primary purpose of these requirements is to protect the rights and privacy of U.S. persons. The sum of these requirements is captured

^{4 (}U) See footnote 1.

TOP SECRET SUBJECTORY

	in NSA's Legal Compliance and Minimization Procedures, USSID SP0018, which governs the collection, retention, and dissemination of signals intelligence.
Applicable Policies, Procedures, and Guidelines:	(U) NSA incorporated the laws, regulations and guidelines listed above and other related procedures in an internal document, "Legal Compliance and U.S. Persons Minimization Procedures," also referred to as "U.S. Signals Intelligence Directive SP0018" or "USSID SP0018." These minimization procedures govern the entire process NSA follows when collecting, processing, retaining, and disseminating foreign intelligence that may contain U.S. person information. All NSA employees working with signals intelligence data are required to complete training to keep them abreast of legal requirements.
	(U) In addition to the laws, regulations, and guidelines that are implemented via USSID SP0018, the NSA adheres to Presidential Policy Directive No. 28 (PPD-28), which provides further policy direction for the United States' conduct of signals intelligence activities. Among other things, PPD-28 requires that the United States' signals intelligence activities "include appropriate safeguards for the personal information of all individuals To the maximum extent feasible consistent with national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality."

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

	<i>NSA Classified</i> Data Mi his table is classified GECRET//	ning Activity #5	
T	his table is classified GECRET#	SMREE TO USA, TVET	1
Tide	(II/FOHO)		;
Title:	(U/ Teue)	:	;
Description:	(C//CI//DEL TO UCA EVEV)	;	1
Description.			1
	ı	:	
		ž.	
=		i.	
15			1
			1
		:	1:
Α .		<u>;</u> ;	
		5	
		•	
		;;	
		11	
	(S//SI//REL TO USA, FVEY)		.:
	(on sintell to obti, i ver)		ť:
		1	[:
	5	•	ŀ
		•	1
	×	•	F
		, a	1
			17
		:	1
	× -	<u>.</u>	1
		•	1:
Tarlanda	(C//C//DEL TO LICA EVEN)		4
Technology Used:	(C//CL//REL TO USA, FWEY)	•	4
Used.		:	1
		: :	
		: :	ľ
Data Sources:	(SHOWNEL TO USALTYEY)		4
			T.
1		:	:
Efficacy		No. 32 (A)	1:
Assessment:			1

TOR CECRET/CUAIOCORN

Privacy Impact	(U) Given that there are no changes to the activity, the 2016 assessment
Assessment:	remains valid:
	j
	(U) Using the civil liberties and privacy assessment process described in
	the Background section, this activity has the following impacts and
	employs the following safeguards:
	(U) This data mining activity is not intended to uncover patterns known to
	be engaged in by U.S. persons.
	be engaged in by C.S. persons.
	(TC//CL//DEL TO LIGH FURTY)
	, , , , , , , , , , , , , , , , , , , ,
	1 65 1
<i>i.</i>	
	1 1:10
	1 501
	5 93.0
	(TC//CU//DEL TO UCA, EVEV)
	H : [3]
	: :1
	1
	/TC//CL//DEL TO LICA EVENO
	l t
	[: [·]
	l : []
	l : : : : : : : : : : : : : : : : : : :
	I : I
2	
	(TS//SI//DEL TO USA, FVEY)
7	
	2

	also protects the privacy rights of U.S. persons through its minimization procedures. Section 2.3 of E.O. 12333, as amended, specifies that elements of the Intelligence Community are authorized to collect, retain, or disseminate information concerning U.S. persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General, after consultation with the Director of National Intelligence. NSA adheres to the limitations that are contained within those procedures and abides by the restrictions in its Attorney General-approved procedures specifically designed to provide protection to the privacy of U.S. persons. Pursuant to PPD-28, NSA implemented supplemental procedures extending comparable safeguards to all individuals, regardless of nationality.
	(TS://SI//REL TO USA, FVEY) In order to further reduce the civil liberties and privacy impacts associated with this activity, key safeguards include: controlled access to users with completed training, documented justification for queries, auditing, dissemination restrictions to only that which is relevant for foreign intelligence or counterintelligence purposes, and retention limited to five years unless it has been specifically determined to be relevant for foreign intelligence or counterintelligence.
Governing Laws and Regulations:	(U) Section 1.7(c) of E.O. 12333 authorizes the Director, NSA to collect, process, analyze, produce, and disseminate signals intelligence for foreign intelligence and counterintelligence purposes to support national and departmental missions. The Secretary of Defense issued required procedures known as DoD Regulation 5240.1-R (Procedures Governing the Activities of DoD Intelligence Components That Affect United States Persons) and its Classified Annex. ⁵ Furthermore, NSA's signals intelligence activities must comply with the Fourth Amendment to the U.S. Constitution. The primary purpose of these requirements is to protect the rights and privacy of U.S. persons. The sum of these requirements is captured in NSA's Legal Compliance and Minimization Procedures, USSID SP0018, which governs the collection, retention, and dissemination of signals intelligence.
Applicable Policies, Procedures, and Guidelines:	(U) NSA incorporated the laws, regulations and guidelines listed above and other related procedures in an internal document, "Legal Compliance and U.S. Persons Minimization Procedures," also referred to as "U.S. Signals Intelligence Directive SP0018" or "USSID SP0018." These

⁵ (U) See footnote 1.

TOP SECRET SUMOTORS

minimization procedures govern the entire process NSA follows when collecting, processing, retaining, and disseminating foreign intelligence that may contain U.S. person information. All NSA employees working with signals intelligence data are required to complete training to keep them abreast of legal requirements.

(U) In addition to the laws, regulations, and guidelines that are implemented via USSID SP0018, the NSA adheres to Presidential Policy Directive No. 28 (PPD-28), which provides further policy direction for the United States' conduct of signals intelligence activities. Among other things, PPD-28 requires that the United States' signals intelligence activities "include appropriate safeguards for the personal information of all individuals... To the maximum extent feasible consistent with national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality."

(b) (1)

(b) (3) -18 USC 798

(b) (3) -50 USC 3024(i)

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

This	NSA Classified Data Mining Activity #6 stable is classified TOP SECRET//SL//REL TO USA, FYEY
Title:	(U// EQUO)
Description:	(TSI/SI/REL TO USA, TVET)
Technology Used:	(TS//SI/REL TO USA, FVEY)
Data Sources:	(TS//SI//REL TO USA, TVET)
Efficacy Assessment:	(TS//SI//REL TO USA, FVEY)
Privacy Impact Assessment:	(U) Given that there are no changes to the activity, the 2016 assessment remains valid: (U) Using the civil liberties and privacy assessment process described in the Background section, this activity has the following impacts and employs the following safeguards: (U) This data mining activity is not intended to uncover patterns known to be engaged in by U.S. persons.

individuals, regardless of nationality.

to the privacy of U.S. persons. Pursuant to PPD-28, NSA implemented supplemental procedures extending comparable safeguards to all

TOT SECRETIFICATION

(b)(3)-P.L. 86-3	include: controlled access to users with completed training, documented justification for queries, auditing, dissemination restrictions to only that which is relevant for foreign intelligence or counterintelligence purposes, and retention limited to five years unless it has been specifically determined to be relevant for foreign intelligence or counterintelligence. With respect to this activity
Governin	g Laws (U) Section 1.7(c) of E.O. 12333 authorizes the Director, NSA to collect,
and Regu	(Manager and Manager and Mana
Applicab Policies, Procedure Guideline	and other related procedures in an internal document, "Legal Compliance s, and U.S. Persons Minimization Procedures," also referred to as "U.S.

THE PARTY OF THE P

security, these policies and procedures are to be applied equally to the
personal information of all persons, regardless of nationality."

UNCLASSIFIED//FORCETTE CSE CITET

National Security Agency

(U) Federal Agency Data Mining Report for Fiscal Year (FY) 2018

(U) Introduction.

(U) The National Security Agency (NSA) has prepared this report in response to Section (c)(3)(A) of Section 804, Public Law 110-53, Federal Agency Data Mining Reporting Act of 2007 (the Act) to address the data mining activities conducted at NSA during Fiscal Year 2018. This report will be made available to those entities required under Section (c)(3)(B) of the Act.

(U) Background.

- (U) Pursuant to its mission, NSA uses and develops communications data mining techniques for foreign intelligence purposes, including detection of terrorist activity.
- (U) NSA researches the use of commercial and academic data mining techniques to advance its authorized foreign intelligence mission through the science of discovery. The goal is to use the patterns of a target group's activity to identify previously unknown foreign terrorists, foreign intelligence officers, etc. within legally gathered foreign intelligence information.
- (U#FOLIO) This report was completed by all Directorates at NSA and compiled by the NSA Office of Civil Liberties, Privacy and Transparency, the Legislative, State and Local Affairs Office, and the Office of the General Counsel. The data mining activities in this 2018 report are the same or similar to activities that were in the previous year's report; however, due to consolidation of efforts and changing requirements, some analytics are scheduled to transition to other programs and/or will be decommissioned. These changes have been noted in this year's report. NSA's Civil Liberties and Privacy Assessment (CLPA) process remains consistent. As noted in the 2017 report, NSA's CLPA process describes the relevant facts using four categories of questions to assess the level of impact on individuals:
 - How intrusive/comprehensive is the activity based on the data type(s)?
 - How intentionally broad is the activity based on the scope of persons in the data?
 - How unspecified/expansive is the activity based on the operational purpose and use of the data?
 - How imprecise/inaccurate is the activity's methodology to achieve the operational purpose?
- (U//Febb) The CLPAs then describe the safeguards that NSA implements to mitigate and reduce these impacts.
- (U//POUC) In January 2015, NSA adopted written supplemental procedures to formally implement Presidential Policy Directive No. 28 (PPD-28). NSA CLPAs contained in this report assess impacts on all individuals, regardless of nationality, in accordance with PPD-28.

TOT SECRETIFICATION

National Security Agency

(U) Federal Agency Data Mining Report for Fiscal Year (FY) 2018 Classified Annex

(U) Introduction.

(U) The National Security Agency (NSA) has prepared this Annex in compliance with Section (c)(3)(A) of Section 804, Public Law 110-53, Federal Agency Data Mining Reporting Act of 2007 (the Act) to address the classified data mining activities conducted at NSA during Fiscal Year 2018. This Annex will be made available to those entities required under Section (c)(3)(B) of the Act.

(U) Background.

- (U) Pursuant to its mission, NSA uses and develops communications data mining techniques for foreign intelligence purposes, including detection of terrorist activity.
- (U) NSA researches the use of commercial and academic data mining techniques to advance its authorized foreign intelligence mission through the science of discovery. The goal is to use the patterns of a target group's activity to identify previously unknown foreign terrorists, foreign intelligence officers, etc. within legally gathered foreign intelligence information.
- (U/Feue) This report was completed by all Directorates at NSA and compiled by the NSA Office of Civil Liberties, Privacy and Transparency, the Legislative, State and Local Affairs Office, and the Office of the General Counsel. The data mining activities in this 2018 report are the same or similar to activities that were in the previous year's report; however, due to consolidation of efforts and changing requirements, some analytics are scheduled to transition to other programs and/or will be decommissioned. These changes have been noted in this year's report. NSA's Civil Liberties and Privacy Assessment (CLPA) process remains consistent. As noted in the 2017 report, NSA's CLPA process describes the relevant facts using four categories of questions to assess the level of impact on individuals:
 - How intrusive/comprehensive is the activity based on the data type(s)?
 - How intentionally broad is the activity based on the scope of persons in the data?
 - How unspecified/expansive is the activity based on the operational purpose and use of the data?
 - How imprecise/inaccurate is the activity's methodology to achieve the operational purpose?

(U//Feue) The CLPAs then describe the	safeguards that NSA implements to mitigate and
reduce these impacts.	

Classified By
Derived From: NSAM 1-52
Dated: 20180110
Declassify On:

TOP SECRETUSIANOFORM

(U//POUO) In January 2015, NSA adopted written supplemental procedures to formally implement Presidential Policy Directive No. 28 (PPD-28). NSA CLPAs contained in this report assess impacts on all individuals, regardless of nationality, in accordance with PPD-28.

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

(U) NSA Classified Report for FY2018.

	NSA CI	lassified Data M	ining Activity #1			. 3
	This table is c	lassified TOP SI	CILCIIIOIIIIOI	CONV		
Title:	(U// FOUO)			:		
Description:	(TS//SL/NT)			•	: 1	
					:	
	#					
	(TS//SL/AIF)			**	<u> </u>	-
	(Ibhishiri)			:	:	1
	^			::	:	
				::	:	
				<u>:</u>	÷	
Technology Used:	(TS//SI//REL-1	O USA, TVEY)	•	:	
				-]
Data Sources:	(TO/OL/DELE	O USA, FVEY		•		İ
Efficacy	(TS//SI/AIF)					
Assessment:						
			100000000000000000000000000000000000000			

(TS//SI//REL TO USA, FVEY)

		(710000	
DO	JID.	0/19200)
(k	0) (3	3)-P.L.	86-36

OP OF OPPT OF MOTORY

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

(U// FOUO) Safeguards:	
	NSA
procedures. Section 2.3 of of the Intelligence Comm disseminate information of procedures established by by the Attorney General (National Intelligence (DN contained within those prapproved procedures, whit to the privacy of U.S. per	s of U.S. persons through its minimization of E.O. 12333, as amended, specifies that elements unity (IC) are authorized to collect, retain, or concerning U.S. persons only in accordance with the head of the agency concerned and approved (AG), after consultation with the Director of WI). NSA adheres to the limitations that are occedures and abides by the restrictions in its AGich are specifically designed to provide protection sons. Pursuant to PPD-28, NSA implemented extending comparable safeguards to all nationality.

Governing Laws and Regulations:

(U) NSA activities must comply with the Fourth Amendment to the U.S. Constitution. Section 1.7(c) of E.O. 12333 authorizes the Director, NSA to collect, process, analyze, produce, and disseminate SIGINT for foreign intelligence and counterintelligence purposes to support national and departmental missions. The Secretary of Defense issued required minimization procedures known as DoD Manual 5240.01 (Procedures Governing the Conduct of DoD Intelligence Activities) and its Classified Annex. The sum of these requirements is captured in an internal document, "Legal Compliance and U.S. Persons Minimization

¹ (U) Note that, effective 8 August 2016, the Secretary of Defense, in coordination with the Director of National Intelligence and with the approval of the Attorney General, issued DoD Manual 5240.01 to govern the conduct of DoD intelligence activities. DoDM 5240.01 supersedes Procedures 1-10 in DoD 5240.01-R. DoDD 5148.13 subsequently superseded DoD 5240.01-R Procedures 14 and 15 Procs. Procedures 11-13 of DoD 5240.01-R remain in effect. Additionally, the Classified Annex remains in effect until updated or superseded.

	Procedures," also referred to as "U.S. Signals Intelligence Directive SP0018" or simply "USSID SP0018," which governs the collection, processing, retention, and dissemination of SIGINT. The primary purpose of these requirements is to protect the rights and privacy of U.S. persons.
Applicable Policies, Procedures, and Guidelines:	(U) NSA incorporated the laws, regulations, and guidelines listed in the Governing Laws and Regulations portion of this table and other related procedures in USSID SP0018. These minimization procedures govern the entire process NSA follows when collecting, processing, retaining, and disseminating foreign intelligence that may contain U.S. person information. All NSA affiliates working with SIGINT data are required to complete mandatory training to keep them abreast of legal requirements. (U) In addition to the laws, regulations, and guidelines that are implemented via USSID SP0018, NSA adheres to PPD-28, which provides further policy direction for the United States' conduct of SIGINT activities. Among other things, PPD-28 requires that the United States' SIGINT activities "include appropriate safeguards for the personal information of all individualsTo the maximum extent feasible, consistent with national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality."

	NSA Classified Data Mining Activity #2 This table is classified TCP SECRET//SE//NOPS) Rij	
Title:	(U// Peus)		ē.
Description:	(C//CL//PEL TO USA, FVEY)	***************************************	
	(C//CL//REL TO USA, FVEY)		1
	(C//CL//REL TO USA, FVEY)]
Technology Used:	(C//REL TO USA, FVEY)	:	
	(SHSHIREL TO USA, TVEY)		

	(TCUCLUDEL TO LICA TURE)
	(TOHOMITEDE TO CORE, I VET)
	1 9 81
	1 8
	1 3 51
	· · · · · · · · · · · · · · · · · · ·
	1 10 10
	(S//SL/REL TO USA, TVET)
	1 11 41
	1 31
V 1	1 31
Data Sources:	(TC//CI/AT)
	1 4
	1 : 31
	1
	8 39
	<u> </u>
Efficacy	(MOLIGILIA DI TOLLICA DI INVI)
	(TOHOLHREE TO CON, I VET)
Assessment:	A section of the sect
	•

	(CUCIUDE) TO VICE DIVIDIO
	(SHOPPICE TO CON, I VET)
V A2	
,	
Privacy Impact	(U) Using the CLPA process described in the Background section, this
Assessment:	activity has the following impacts and employs the following safeguards:
en ed Edit G. 1940 jeur G.	mpass and employs the following safeguards.
	(U) This data mining activity is not intended to uncover patterns known to
	be engaged in by U.S. persons.
	or thought in of clo. persons.

(U//FOUO)

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

NSA also

protects the privacy rights of U.S. persons through its minimization procedures. Section 2.3 of E.O. 12333, as amended, specifies that elements of the IC are authorized to collect, retain, or disseminate information concerning U.S. persons only in accordance with procedures established by the head of the agency concerned and approved by the AG, after consultation with the DNI. NSA adheres to the limitations that are contained within those procedures and abides by the restrictions in its AG-approved procedures specifically designed to provide protection to the privacy of U.S. persons. Pursuant to PPD-28, NSA implemented supplemental procedures extending comparable safeguards to all individuals, regardless of nationality.

(TS//SI/REL TO USA, FVEY) In order to further reduce the CLP impacts associated with this activity, key safeguards include: controlled access to users with completed training, documented justification for queries, auditing, dissemination restrictions to only that which is relevant for foreign intelligence or counterintelligence purposes, and retention limited to 5 years unless it has been specifically determined to be relevant for foreign intelligence or counterintelligence. The impact of this activity is also mitigated by the masking of U.S. and Second Party person results whenever they can be identified.

Governing Laws and Regulations:

(U) NSA activities must comply with the Fourth Amendment to the U.S. Constitution. Section 1.7(c) of E.O. 12333 authorizes the Director, NSA to collect, process, analyze, produce, and disseminate SIGINT for foreign intelligence and counterintelligence purposes to support national and departmental missions. The Secretary of Defense issued required minimization procedures DoDM 5240.01 and its Classified Annex.² The sum of these requirements is captured in USSID SP0018, which governs the collection, processing, retention, and dissemination of SIGINT. The primary purpose of these requirements is to protect the rights and privacy of U.S. persons.

Applicable Policies, Procedures, and Guidelines:

(U) NSA incorporated the laws, regulations, and guidelines listed above and other related procedures in USSID SP0018. These minimization procedures govern the entire process NSA follows when collecting, processing, retaining, and disseminating foreign intelligence that may contain U.S. person information. All NSA affiliates working with SIGINT data are required to complete mandatory training to keep them abreast of legal requirements.

² (U) See footnote 1.

(U) In addition to the laws, regulations, and guidelines that are implemented via USSID SP0018, NSA adheres to PPD-28, which provides further policy direction for the United States' conduct of SIGINT activities. Among other things, PPD-28 requires that the United States' SIGINT activities "include appropriate safeguards for the personal information of all individuals... To the maximum extent feasible consistent with national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality."

Doc ID: 6719288

TOT SECRETISHINGTORN

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

	NSA Classified Data Mining Activity #3	
TI	NSA Classified Data Mining Activity #3 nis table is classified TOP SECRET//SE//REL TO U	CLITTEY
itle:	(TO VOLUME)	
nic.	(TOPOTPICE TO COA, I VET)	
		(:
Description:	(S//SI//REL TO USA, TVEY)	*
escription.	(SHSINIED TO USIL, TVDT)	
	·	Ĭ: :
		<i>t</i> : :
		\ ; :
		' : :
	(S//SI//REL TO USA, IVEY)	} :
) []
		3 []
		3 19
		- { - }
		13
	1	13
		- 3
		3
echnology sed:	(S//SI/REL TO USA, FVET)	· .
seu.		3
	(; I
		3 1
	:	
		4
	(CHOLINGL TO USA, FVEY)	
		·
		. 11
		• 11
		•
	(S//SI//REL TO USA, I VET)	
		7
	1	

TOP SECRET SUPPOSED !

TOP OF OPEN CALL TOP OP A

(b) (3) -P.L. 86-36	(b) (3)-18 USC 798 (b) (3)-50 USC 3024(i)
	(b) (3)-P.L. 86-36
	noted, the purpose and uses are controlled through documented foreign intelligence/counterintelligence justifications for queries and auditing. (TS//SH/REL TO USA, TVET)
	(TOMODYRED TO GOT, TYDY)
	ALUTONO CO.
	protects the privacy rights of U.S. persons through its minimization procedures. Section 2.3 of E.O. 12333, as amended, specifies that elements of the IC are authorized to collect, retain, or disseminate information concerning U.S. persons only in accordance with procedures established by the head of the agency concerned and approved by the AG, after consultation with the DNI. NSA adheres to the limitations that are contained within those procedures and abides by the restrictions in its AG-approved procedures specifically designed to provide protection to the privacy of U.S. persons. Pursuant to PPD-28, NSA implemented supplemental procedures extending comparable safeguards to all individuals, regardless of nationality.
	(TS://SI//DEL TO USA, FYEY) In order to further reduce the CLP impacts associated with this activity, key safeguards include: controlled access to users with completed training, documented justification for queries,

auditing, dissemination restrictions to only that which is relevant for foreign intelligence or counterintelligence purposes, and retention limited

(b) (1)

	to 5 years unless it has been specifically determined to be relevant for foreign intelligence or counterintelligence.
Governing Laws and Regulations:	(U) NSA activities must comply with the Fourth Amendment to the U.S. Constitution. Section 1.7(c) of E.O. 12333 authorizes the Director, NSA to collect, process, analyze, produce, and disseminate SIGINT for foreign intelligence and counterintelligence purposes to support national and departmental missions. The Secretary of Defense issued required minimization procedures DoDM 5240.01 and its Classified Annex. ³ The sum of these requirements is captured in USSID SP0018, which governs the collection, processing, retention, and dissemination of SIGINT. The primary purpose of these requirements is to protect the rights and privacy of U.S. persons.
Applicable Policies, Procedures, and Guidelines:	(U) NSA incorporated the laws, regulations, and guidelines listed above and other related procedures in USSID SP0018. These minimization procedures govern the entire process NSA follows when collecting, processing, retaining, and disseminating foreign intelligence that may contain U.S. person information. All NSA affiliates working with SIGINT data are required to complete mandatory training to keep them abreast of legal requirements.
	(U) In addition to the laws, regulations, and guidelines that are implemented via USSID SP0018, NSA adheres to PPD-28, which provides further policy direction for the United States' conduct of SIGINT activities. Among other things, PPD-28 requires that the United States' SIGINT activities "include appropriate safeguards for the personal information of all individuals To the maximum extent feasible consistent with national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality."

15

³ See footnote 1.

(b) (1)

	NSA Classified Data Mining Activity #4 This table is classified TOP SECRET//SI//NOPORM	
	This table is classified for SECRETIFICATION ON T	
Title:	(TS//SI//REL TO USA, FVEY)	لہ
	:	
	:	
		∐ [3
Description:	(SI/SI/INDE TO USA, I VET)	
		1
	:	et de la companya de
	:	
	<u>:</u>	
	:	
	;	3
	l	
	:	
	(CUCYUDDY TO YYO L DY DY	1
	GHORINEL TO COM, I VET	4
1		
		E
r		
		:
Technology Used:	(TS//SI//REL TO USA, FVEY)	+
zoomieregy esou.	(ISMSERIED TO CSI, I VET)	4
	λ	ŀ
	×	ŀ
_	*	ſ
		}
		_}
÷ _n	(TS//SI//REL TO USA, I VET)	H
*		

Doc ID: 6719288

TOR CEORET WOLLD TOPON

	[·		
	•		
	(TOUGH DEL TO LIGH DIVERN)		
Data Sources:			
	•		
	l : I !		
	l : I 🛚		
180			
Efficacy	The state of the s		
	OHOURED TO COM, I VEI		
Assessment:			
	and the second s		
	• • •		
	(TOUGHARI TO HOLDEN)		
	(ISHSTREE TO CORET VET)		
	l t		
2.1			
Privacy Impact	(U) Given that there are no changes to the activity, the 2017 assessment		
Assessment:			
Assessment.	remains valid:		
	(U) Using the CLPA process described in the Background section, this		
	activity has the following impacts and employs the following safeguards:		
	are the following impacts and employs the following suregulards.		
27	(U) This data mining activity is not intended to uncover patterns known to-		
	be engaged in by U.S. persons.		
	TOUGH DEL TO LICA EVEN		
- 1	(TONOLITEDE TO COLL, T. P. T.)		
α =			
	×		

TOT SECRETI/SI/NOTOKIN

(b)	(1)		
(b)	(3)-18 U	SC 7	98
(b)	(3)-50 U	SC 3	024(i)
(b)	(3) - P.L.	86-	36

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

	(10//01//101)	
:		•
:		÷
•	(TS//SI//REL TO US/1, FVEY) Purpose: The use of this activity is to	٠.
:	track targets and discover new targets in support of a variety of foreign	
•		
•	intelligence and counterintelligence needs.	
	(TO O O	
*		-
int. •:	ž.	
	7	ŀ
•		I
•	:	ı
•	:	H
•		- 1
•	<u> </u>	_
•	(TSI/SI/IKEE TO COA, TVET)	
	The property of the property of the state of	
		_
*		
		- 1
:		
•		-1
		- 1
	(U //FQUQ) Safeguards:	1
		1
		1
1	NSA	-4
7	also protects the privacy rights of U.S. persons through its minimization	
	procedures. Section 2.3 of E.O. 12333, as amended, specifies that	
	elements of the IC are authorized to collect, retain, or disseminate	
	information concerning U.S. persons only in accordance with procedures	3
	established by the head of the agency concerned and approved by the AC	Ì,
	after consultation with the DNI. NSA adheres to the limitations that are	
	contained within those procedures and abides by the restrictions in its	
	AG-approved procedures specifically designed to provide protection to	
	the privacy of U.S. persons. Pursuant to PPD-28, NSA implemented	
	supplemental procedures extending comparable safeguards to all	
	individuals, regardless of nationality.	
	, 0	
	(TS//SL//REL TO USA, FVEV) In order to further reduce CLP impacts	
	associated with this activity have a few division land at the second at	
	associated with this activity, key safeguards include: controlled access to)

users with completed training, documented justification for queries. auditing, dissemination restrictions to only that which is relevant for foreign intelligence or counterintelligence purposes, and retention limited to five years unless it has been specifically determined to be relevant for foreign intelligence or counterintelligence. In addition, all queries conducted by analysts under this activity are subject to auditing and review to validate both the appropriateness of the query conduced and the foreign intelligence or counterintelligence need. (U) NSA activities must comply with the Fourth Amendment to the U.S. Governing Laws Constitution, and must be conducted in accordance with FISA. Section and Regulations: 1.7(c) of E.O. 12333 authorizes the Director, NSA to collect, process, analyze, produce, and disseminate SIGINT for foreign intelligence and counterintelligence purposes to support national and departmental missions. The Secretary of Defense issued required minimization procedures DoDM 5240.01 and its Classified Annex. 4 The sum of these requirements is captured in USSID SP0018, which governs the collection, processing, retention, and dissemination of SIGINT. The primary purpose of these requirements is to protect the rights and privacy of U.S. persons. Applicable (U) NSA incorporated the laws, regulations and guidelines listed above and other related procedures in USSID SP0018. These minimization Policies, Procedures, and procedures govern the entire process NSA follows when collecting, Guidelines: processing, retaining, and disseminating foreign intelligence that may contain U.S. person information. All NSA affiliates working with SIGINT data are required to complete mandatory training to keep them abreast of legal requirements. (U) In addition to the laws, regulations, and guidelines that are implemented via USSID SP0018, the NSA adheres to PPD-28, which provides further policy direction for the United States' conduct of SIGINT activities. Among other things, PPD-28 requires that the United States' SIGINT activities "include appropriate safeguards for the personal information of all individuals... To the maximum extent feasible consistent with national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality."

^{4 (}U) See footnote 1.

Doc ID: 6719288

	NSA Classified Data Mining Activity 45		
7	NSA Classified Data Mining Activity #5 This table is classified CECRET//SI//REL TO USA, FV		
	his table is classified becker mounted to obtt, i v		
Title:	(U/ /Teue)		,
11110.	(6/2000)		`
Description:	(CHSHIREL TO USA, TVEY)	5.5	1
			{
			₹ -
	, , , , , , , , , , , , , , , , , , ,		
			∛ ∥ ⋅
			3 3
		i I	* :
			3 1
1	1		
	[
	1		
	[
5			
	(CUCUDEL TO LICA EVEN)	10.40 - 0.50	1 :
		n svenski sintosom nijos jin	
	· · · · · · · · · · · · · · · · · · ·		
	<u> </u>		
	<u> </u>		
	1		
Technology	(CUCUREL TO USA, FVEY)		The second
Used:			
	j		
Data Sources:	(S//SI/REL TO USA, FVEY)		
Data Sources.	(SHSHILLE TO CSIL, I VEF)		
	:		:
		. /o	
Efficacy	(SHSHREE TO USA, FVEY)		
Assessment:			

TOP SECRETION AND ONLY

(b) (1) (b) (3) -18 USC 798 (b) (3) -50 USC 3024(i)

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

Privacy Impact Assessment: (U) Using the CLPA process described in the Background section; this activity has the following impacts and employs the following safeguards: (U) This data mining activity is not intended to unover patterns known to be engaged in by U.S. persons. (TE//GL/REL TO U.S., TVEY) (E//GL/REL TO U.S., TVEY) (TE//GL/REL TO U.S., TVEY)		
Assessment: activity has the following impacts and employs the following safeguards: (U) This data mining activity is not intended to unever patterns known to be engaged in by U.S. persons. (TEMELITO USA, FVEY) (EMELITO USA, FVEY) (TEMELITO USA, FVEY)		
Assessment: activity has the following impacts and employs the following safeguards: (U) This data mining activity is not intended to unever patterns known to be engaged in by U.S. persons. (TEMELITO USA, FVEY) (EMELITO USA, FVEY) (TEMELITO USA, FVEY)		
Assessment: activity has the following impacts and employs the following safeguards: (U) This data mining activity is not intended to unever patterns known to be engaged in by U.S. persons. (TEMELITO USA, FVEY) (EMELITO USA, FVEY) (TEMELITO USA, FVEY)		
(TS//SW/REL TO USA, FVEY) (TS//SW/REL TO USA, FVEY)		
(TS//SW/REL TO USA, FVEY) (TS//SW/REL TO USA, FVEY)		
(TE//SW/REL TO USA, FVEY) (S//SW/REL TO USA, FVEY)		
(TS//SW/REL TO USA, FVEY) (TS//SW/REL TO USA, FVEY)		be engaged in by U.S. persons.
(TS//SI//REL TO USA, FVEY)		
(TS//SE//REL TO USA, FVEY)		(All and All a
(TC//CL//DEL TO UCA, FVEY)		
(TC//CI//DEL TO USA, FVEY)		(TC//CI//REL TO UCA, EVEY)
(TC//CI//DEL TO USA, FVEY)	= , 2 2	
(TC//CI//DEL TO USA, FVEY)		(AHAMA DA DA MA DA
		(SIISIIIKEE TO OSIA, TVET)
		[F:
	(A)	
(TS//SL/REL TO USA, TVET)		(TC//CI//DEL TO LICA EVEN)
(TS//SI//REL TO USA, TVET)		(13733132313 3313,1121)
(TS//SL/REL TO USA, TVET)		
(TS//SI//REL TO USA, TVET)		
(TS//SI//REL TO USA, TVET)		· II
(TS//SI//REL TO USA, TVET)		
(TS//SI//REL TO USA, TVET)		
(TS//SI//REL TO USA, TVET)		•
(TS//SI//REL TO USA, TVLT)		
		(TS//SI//REL TO USA, TVET)
	2	

(U//FeUe) Safeguards: also protects the privacy rights of U.S. persons through its minimization procedures. Section 2.3 of E.O. 12333, as amended, specifies that elements of the IC are authorized to collect, retain, or disseminate information concerning U.S. persons only in accordance with procedures established by the head of the agency concerned and approved by the AG, after consultation with the DNI. NSA adheres to the limitations that are contained within those procedures and abides by the restrictions in its AG-approved procedures specifically designed to provide protection to the privacy of U.S. persons. Pursuant to PPD-28, NSA implemented supplemental procedures extending comparable safeguards to all individuals, regardless of nationality. (TS//ST/PEL TO USA, FVEY) In order to further reduce the CLP impacts associated with this activity, key safeguards include: controlled access to users with completed training, documented justification for queries. auditing, dissemination restrictions to only that which is relevant for foreign intelligence or counterintelligence purposes, and retention limited to 5 years unless it has been specifically determined to be relevant for foreign intelligence or counterintelligence. Governing Laws (U) NSA activities must comply with the Fourth Amendment to the U.S. and Regulations: Constitution. Section 1.7(c) of E.O. 12333 authorizes the Director, NSA to collect, process, analyze, produce, and disseminate SIGINT for foreign intelligence and counterintelligence purposes to support national and departmental missions. The Secretary of Defense issued required minimization procedures DoDM 5240.01 and its Classified Annex. 5 The sum of these requirements is captured in USSID SP0018, which governs the collection, processing, retention, and dissemination of SIGINT. The primary purpose of these requirements is to protect the rights and privacy of U.S. persons. Applicable (U) NSA incorporated the laws, regulations and guidelines listed above and other related procedures in USSID SP0018. These minimization Policies. Procedures, and procedures govern the entire process NSA follows when collecting. Guidelines: processing, retaining, and disseminating foreign intelligence that may contain U.S. person information. All NSA affiliates working with SIGINT data are required to complete mandatory training to keep them abreast of legal requirements.

⁵ See footnote 1.

TOP SECRET//SI//NOFORN

(U) In addition to the laws, regulations, and guidelines that are implemented via USSID SP0018, the NSA adheres to PPD-28, which provides further policy direction for the United States' conduct of SIGINT activities. Among other things, PPD-28 requires that the United States' SIGINT activities "include appropriate safeguards for the personal information of all individuals... To the maximum extent feasible consistent with national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality."

NSA Classified Data Mining Activity #6 This table is classified TOT SECRET//SI//REL TO USA, FVEY		
Title:	(U/ /Peue)	
Description:	(TS//SI//REL TO USA, FVET)	
	* * * * * * * * * * * * * * * * * * *	
Technology Used:	(TS//SI//REL TO USA, FVEY)	
Data Sources:	(TS//SI//REL TO USA, FVEY)	
Efficacy Assessment:	(TS//SI//REL TO USA, FVEY)	
Privacy Impact Assessment:	(U) Given that there are no changes to the activity, the 2017 assessment remains valid:	

procedures. Section 2.3 of E.O. 12333, as amended, specifies that elements of the IC are authorized to collect, retain, or disseminate

		•
		information concerning U.S. persons only in accordance with procedures established by the head of the agency concerned and approved by the AG, after consultation with the DNI. NSA adheres to the limitations that are contained within those procedures and abides by the restrictions in its AG approved procedures specifically designed to provide protection to the privacy of U.S. persons. Pursuant to PPD-28, NSA implemented supplemental procedures extending comparable safeguards to all individuals, regardless of nationality.
		(FOURTURE TO LIGHT PURIS)
		s include: controlled access to
		users with completed training, documented justification for queries, auditing, dissemination restrictions to only that which is relevant for foreign intelligence or counterintelligence purposes, and retention limited
(1-) (2) D	7 00 00	to 5 years unless it has been specifically determined to be relevant for
(D) (3)-P.	.L. 86-36	foreign intelligence or counterintelligence. With respect to this activity
	Governing Laws	(U) NSA's activities must comply with the Fourth Amendment to the U.S.
	and Regulations:	Constitution. Section 1.7(c) of E.O. 12333 authorizes the Director, NSA to collect, process, analyze, produce, and disseminate SIGINT for foreign intelligence and counterintelligence purposes to support national and departmental missions. The Secretary of Defense issued required minimization procedures DoDM 5240.1 and its Classified Annex. ⁶ The sum of these requirements is captured in USSID SP0018, which governs the collection, processing, retention, and dissemination of SIGINT. The primary purpose of these requirements is to protect the rights and privacy of U.S. persons.
	Applicable Policies, Procedures, and Guidelines:	(U) NSA incorporated the laws, regulations and guidelines listed above and other related procedures in USSID SP0018. These minimization procedures govern the entire process NSA follows when collecting, processing, retaining, and disseminating foreign intelligence that may contain U.S. person information. All NSA affiliates working with SIGINT data are required to complete mandatory training to keep them abreast of legal requirements.

⁶ (U) See footnote 1.

TOP OF CREATURE IN COLORAL

(U) In addition to the laws, regulations, and guidelines that are implemented via USSID SP0018, the NSA adheres to PPD-28, which provides further policy direction for the United States' conduct of SIGINT activities. Among other things, PPD-28 requires that the United SIGINT activities "include appropriate safeguards for the personal information of all individuals... To the maximum extent feasible consistent with national security, these policies and procedures are to be applied equally to the personal information of all persons, regardless of nationality."