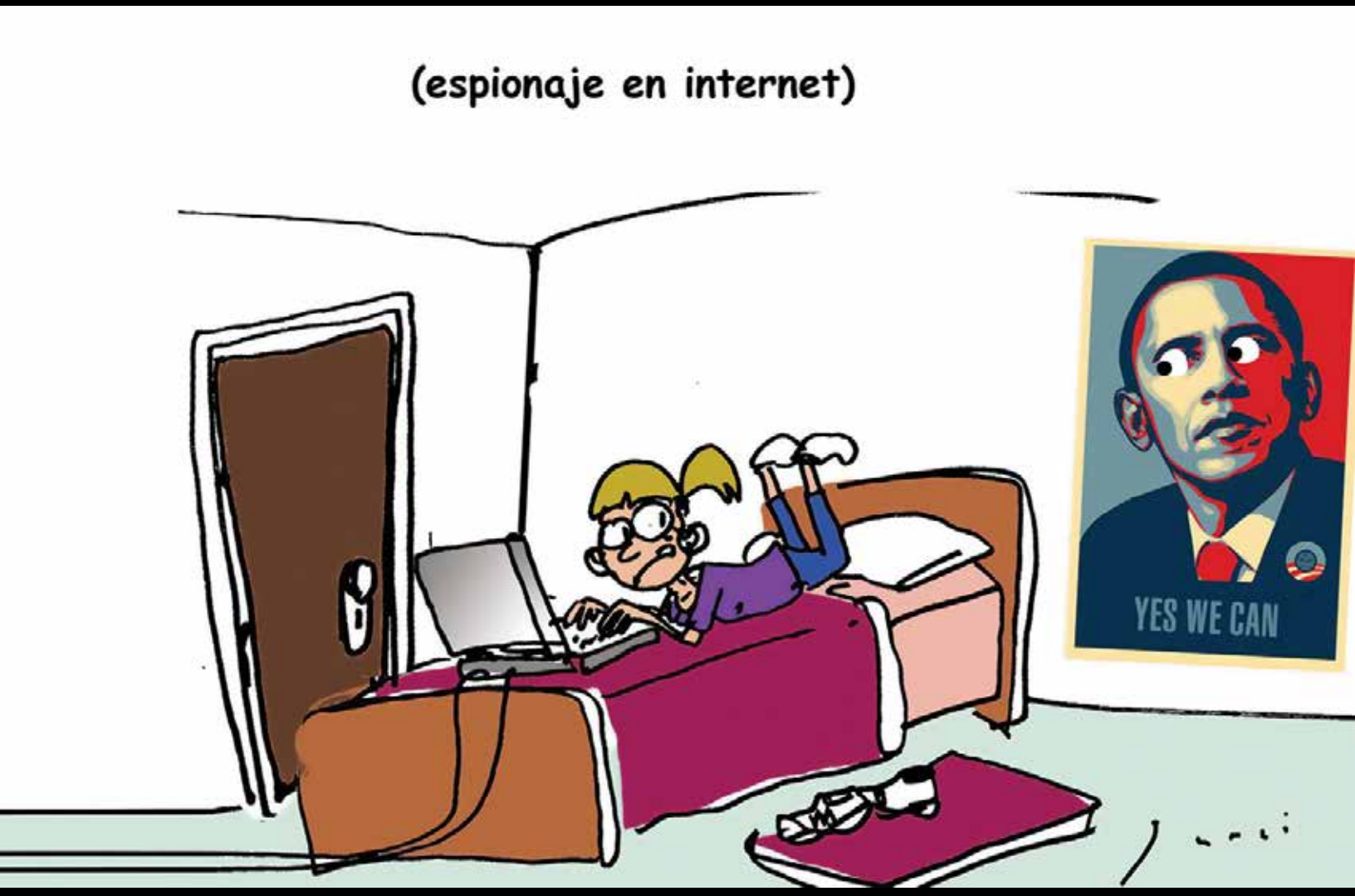
Más del 70% en EU repudia el espionaje interno de Obama



Indice

Encuesta Few See Adequate Limits on NSA Surveillance Program

Más del 70% en EU repudia el espionaje interno de Obama

En Estados Unidos el 70 por ciento de los estadounidenses considera que el presidente Barack Hussein Obama utiliza los datos en la red, internet, redes sociales y llamadas telefónicas para espiar a sus propios ciudadanos, más allá de los esfuerzos para combatir al terrorismo, revela la encuesta Vista de la Proyección de los Límites en la Agencia Nacional de Seguridad (Few See Adequate Limits on NSA Surveillance Program).

Además, en opinión del 56 por ciento de los consultados, la Casa Blanca debe poner límites a esas prácticas ilegales.

La encuesta detalla que los tribunales federales de la Unión Americana no ofrecen límites adecuados sobre los datos telefónicos y de Internet, respecto de las labores de espionaje. Además, puntualiza que el presidente Obama utiliza como parte de sus esfuerzos en la lucha contra el terrorismo esta “estrategia de espionaje”, dentro y fuera de su territorio, pero sin revelarlo a los ciudadanos.

Los datos duros de las encuestas realizadas en la nación que más utiliza dicho espionaje son contundentes. El 63 por ciento de los encuestados considera que Washington debe garantizar el sentido de su información sobre el tema de las comunicaciones y el 27 por ciento cree que Obama sólo se ha referido a rastreo de llamadas y correos electrónicos. Además, el 47 por ciento de los consultados dicen que el gobierno tiene métodos secretos para conocer el contenido de las conversaciones.

Por otra parte, el documento que presenta la encuesta concluye que Obama debe mostrar frialdad y convencer a congresistas demócratas y republicanos de que su gobierno apoya la lucha contra el terrorismo. Dicho análisis justifica porque hay más aceptación entre quienes aprueban estas acciones y quienes las rechazan.

En el apartado denominado “Centro para la población y la prensa” se revela que Obama no goza de toda la aceptación cuando la evidencia más contundente del espionaje es ventilada por el contenido de comunicaciones telefónicas y por internet.

Señala también el documento que los votos del Congreso de los Estados Unidos están divididos, pues hay porcentajes de la Cámara de Representantes que cuestionan severamente esta situación.

Las cifras que ofrece este análisis muestran que el 57 por ciento de los demócratas aprueban, la forma en como investigan el espionaje y el 44 por ciento de los republicanos señalan la injerencia que esto provoca en el ánimo de los estadounidenses. Hay quienes desconocen los mecanismos para investigar ataques o intromisiones.

Detalla que la visión pública de la actividad anti terrorista es compleja y una gran parte cree en la acción, pero no en el fondo de los objetivos de la lucha antiterrorismo de Obama.

Hay quienes creen o piensan que el presidente de los Estados Unidos, entró a una dimensión de retrospección cuando lo que realmente se necesita es mantener e incrementar la credibilidad con base en los esfuerzos “anti crimen”.

Dentro de la encuesta, señala este documento que el 50 por ciento de los consultados desaprueba los instrumentos gubernamentales en la lucha anti terrorismo, a pesar de que los programas para prevenir estos hechos, han fallado en todo y en diferentes épocas.

En la página cuatro del documento señala que dos de cada diez encuestados usan esta información de manera inadecuada, y el 14 por ciento de este universo dicen o creen que por lo general esta información está siendo empleada por lo general solo para propósitos de monitoreo.

La guerra de cifras de la nación más vigilada y monitoreada del planeta es incesante pues cerca del 47 por ciento de los encuestados, dicen estar concentrados en las acciones antiterrorismo.

Los republicados priorizan sobre el tema de la seguridad civil y su libertad en un 58 por ciento y sólo 28 por ciento lo considerada marginado en el año 2010.

Algunos demócratas reconocen el aumento en los porcentajes de los métodos de la lucha contra el terrorismo y hay quienes creen o consideran que los agentes anti-terrorismo tienen cubiertos los derechos de los civiles. Es decir, que 4 de cada 10 demócratas también desaprueban las acciones de espionaje de Obama.

Por último, señala este análisis que la gente joven de Estados Unidos rechaza el espionaje en la lucha del gobierno contra el terrorismo, ya que atenta contra las libertades civiles.

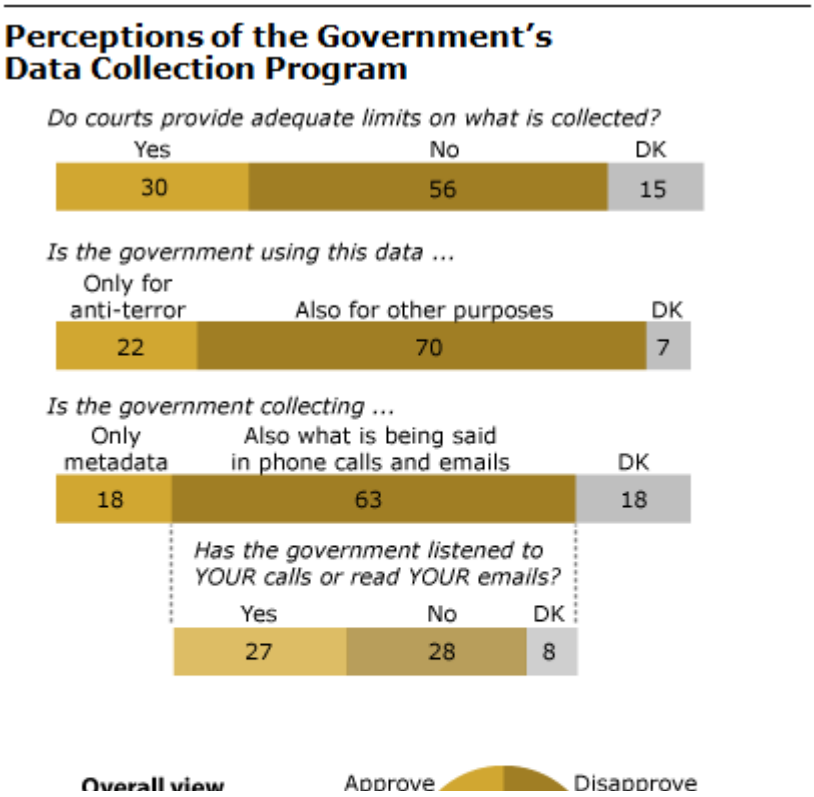
Released: July 26, 2013

Few See Adequate Limits on NSA Surveillance Program

But More Approve than Disapprove

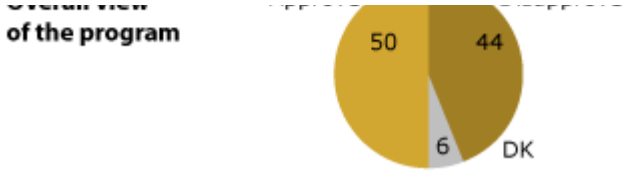
OVERVIEW

A majority of Americans – 56% – say that federal courts fail to provide adequate limits on the telephone and internet data the government is collecting as part of its anti-terrorism efforts. An even larger percentage (70%) believes that the government uses this data for purposes other than investigating terrorism.



And despite the insistence by the president and other senior officials that only "metadata," such as phone numbers and email addresses, is being collected, 63% think the government is also gathering information

about the content of communications – with 27% believing the government has listened to or read *their* phone calls and emails.



PEW RESEARCH CENTER July 17-21, 2013.
Figures may not add to 100% because of rounding.

Nonetheless, the public's bottom line on government anti-terrorism surveillance is narrowly positive. The national survey by the Pew Research Center, conducted July 17-21 among 1,480 adults, finds that 50% approve of the government's collection of telephone and internet data as part of anti-terrorism efforts, while 44% disapprove. These views are little changed from a month ago, when 48% approved and 47% disapproved.

The divisions in public opinion about the government's data-collection program were mirrored in a congressional vote this week on the issue. On July 24, the House of Representatives narrowly defeated an amendment to scale back the NSA's telephone data collection.

Nationwide, there is more support for the government's data-collection program among Democrats (57% approve) than among Republicans (44%), but both parties face significant internal divisions: 36% of Democrats disapprove of the program as do 50% of Republicans.

Government Surveillance: A Question Wording Experiment

The way government surveillance programs are described in public opinion surveys can have a major effect on levels of public support.

To better understand these effects, the Pew Research Center conducted a question-wording experiment in a separate national telephone survey that tested public reactions to four elements of the program:

- Whether metadata or content is being collected
- Whether phone calls or emails are being monitored
- Whether or not the program has court approval
- Whether or not the program is part of anti-terrorism efforts

The results suggest that mention the role of courts, and describe the goal of terrorism reduction, can have a substantial effect on public evaluations.

Public's Divisions Reflected in House Vote on Curbing NSA

Gov't's collection of phone & internet data as part of anti-terrorism efforts ...	Approve	Disapprove	DK
	%	%	%
Total	50	44	6=100
Republican	44	50	6=100
Democrat	57	36	6=100
Independent	47	48	4=100

PEW RESEARCH CENTER July 17-21, 2013. Q21.
Figures may not add to 100% because of rounding.

While views of the program itself are mixed, the debate has raised public concern about whether anti-terror programs are restricting civil liberties.

Overall, 47% say their greater concern about government anti-terrorism policies is that they have gone too far in restricting the average person's civil liberties, while 35% say they are

more concerned that policies have not gone far enough to protect the country. This is the first time in Pew Research polling that more have expressed concern over civil liberties than protection from terrorism since the question was first asked in 2004.

Both Parties Divided in Civil Liberties Concerns over Anti-Terrorism Programs

	Oct 2010		July 2013		Change restrict civ libs
Bigger concern about anti-terror policies	Too far restricting civ libs	Not far enough to protect	Too far restricting civ libs	Not far enough to protect	
	%	%	%	%	
Total	32	47	47	35	+15
Republican	25	58	43	38	+18
Democrat	33	49	42	38	+9
Independent	35	44	52	33	+17

PEW RESEARCH CENTER July 17-21, 2013. Q10.

As concern about civil liberties has grown, the issue now divides members of both parties. Roughly four-in-ten Republicans (43%) and Democrats (42%) say their greater concern over anti-terror policies is that they have gone too far in restricting civil liberties, up sharply from three years ago (25% and 33% in 2010, respectively).

Republicans and Democrats also express similar opinions about news coverage of secret government anti-terrorism programs: Nearly identical percentages in both parties (45% of Democrats, 43% of Republicans) say that the news media should report information it obtains about the secret methods the government uses to fight terrorism, while 51% in each party say it should not.

This marks a change in opinion among both parties since 2006, when Bush administration anti-terror surveillance programs faced scrutiny. In May 2006, a Gallup/USA Today poll found that most Democrats supported news reporting on secret anti-terror programs, while most Republicans said the press should not divulge this information.

Many Who Think Gov't Has Accessed *Their* Data Support the Program

The public's views of the government's anti-terrorism efforts are complex, and many who believe the reach of the government's data collection program is expansive still approve of the effort overall. In every case, however, those who view the government's data collection as far-reaching are less likely to approve of the program than those who do not.

People who believe the government is collecting what is actually being said in emails and phone calls are divided over the overall program: About as many approve (47%) as d isapprove (50%) of the government's

Perceptions of Government's Data

collection of phone and internet data as part of anti-terrorism efforts despite the impression that it is not limited to metadata.

Even among those who believe *their own* communications have been read or listened to, 40% approve of the program, while 58% disapprove.

Of those who say the government is using data for purposes other than to investigate terrorism, 43% approve of the government's data collection; 53% disapprove. Among the small minority (22% of the public) that says the data is only being used to investigate terrorism, 71% approve while just 23% disapprove.

Collection and Views of Program

	View of government data collection program		
	Approve	Dis-approve	DK
	%	%	%
Total	50	44	6=100
Among those who believe ...			
Inadequate court limits	36	62	2=100
Gov't also using data for other purposes	43	53	4=100
Gov't collecting what's actually being said	47	50	3=100
Gov't read/listened to *your* communications	40	58	3=100

PEW RESEARCH CENTER July 17-21, 2013.
Figures may not add to 100% because of rounding.

And those who say federal courts do not place adequate limits on the information the government can collect disapprove of the program by a 62%-36% margin. Conversely, those who say there are adequate limits approve of it, 75%-21%.

Some Suspect Political Motives in Use of Data

A broad majority of the public (70%) believes that the government also is using the data it collects through the NSA program for purposes other than to investigate terrorism. When those who express this view are asked an open-ended question about what other purposes the data is being used for, a range of responses are given, with many focusing on general concerns about government monitoring and spying.

About two-in-ten (19%) say the government is using this data to spy or "be nosy," and another 14% say it is being used for general purposes or monitoring.

But some say the government is collecting

What Other Purposes Is Government Using Data for?

Based on those who say gov't uses data for purposes other than investigating terrorism	July 17-21
	%
To control/spy/be nosy	19
To gather evidence on non-terror crimes	16
General purposes/monitoring	14
Political agenda/targeting	13
Whatever they want	10
Marketing/sell information	2
For protection/national security	2
Tax purposes	1
Targeting interest and religious groups	1
Other targeting/profiling	2
Other	3
Don't know	22

this data for political purposes: 13% say the government has a political agenda, while another 5% say it is being used for general profiling or targeting, to target interest and religious groups or for tax purposes.

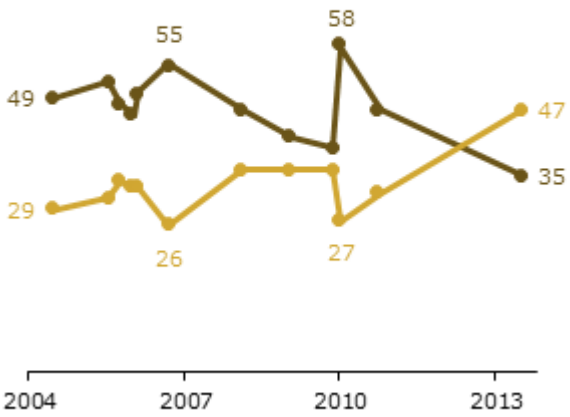
N	978

PEW RESEARCH CENTER July 17-21, 2013. Q24.
Open-ended question; up to three responses accepted.
Based on the 70% of the public who say the government is using the data it collects for purposes other than anti-terror.

Rising Concern over Civil Liberties

Nearly half of Americans (47%) say their greater concern about government anti-terrorism policies is that they have gone too far in restricting the average person's civil liberties; 35% say their greater concern is that they have not gone far enough to adequately protect the country. There has been a 15-point rise in the percentage saying their greater concern is civil liberties since Pew Research last asked the question in October 2010. This is the first time a plurality has expressed greater concern about civil liberties than security since the question was first asked in 2004.

Gov't Anti-Terror Policies Have ...



PEW RESEARCH CENTER July 17-21, 2013. Q10.

The increase in concern about civil liberties has taken place across the board, with double-digit shifts in opinion among nearly all partisan and demographic groups. Republicans prioritized security over civil liberties by a 58%-25% margin in 2010. Today, Republicans are as likely to say their bigger concern is civil liberties (43%) as security

Tea Party Views on Civil Liberties Transformed

	Oct 2010		*July 2013*		
	Too far restricting civ libs	**Not far enough to protect**	**Too far restricting civ libs**	**Not far enough to protect**	**Change in % civ libs**
	%	%	%	%	
Total	32	47	47	35	+15
Republican	25	58	43	38	+18
Conservative	27	57	44	36	+17
Mod/Lib	21	60	41	43	+20
Democrat	33	49	42	38	+9
Liberal	30	55	50	27	+20
Mod/Cons	39	37	38	44	-1
Independent	35	44	52	33	+17
*Among Reps/Rep-leaners**					
Tea Party	20	63	55	31	+35
Not Tea Party	28	51	40	42	+12

PEW RESEARCH CENTER July 17-21, 2013. Q10.
* Based on registered voters

Based on registered voters.

(38%), a balance of opinion nearly identical to that among Democrats (42% civil liberties, 38% security).

While this change has been broad-based, the transformation among Tea Party Republicans stands out. Today, most Republican and Republican-leaning independent voters who agree with the Tea Party are more concerned that government programs are going too far in restricting civil liberties (55%). In October 2010, Tea Party Republican voters by about three-to-one (63% to 20%) said the programs did not go far enough in protecting the country.

Among Democrats and independents, increasing percentages also say their greater concern is that anti-terror policies have curbed civil liberties. About four-in-ten Democrats (42%) express this view, up from 33% three years ago. And the share of independents expressing greater concern over civil liberties has risen 17 points since 2010.

Those under the age of 30 stand out for their broad concern over civil liberties. By about two-to-one (60%-29%) young people say their bigger concern about the government's anti-terrorism policies is that they have gone too far in restricting the average person's civil liberties rather than not going far enough to protect the country.

Young People More Concerned that Anti-Terror Policies Go Too Far in Restricting Civil Liberties

	Oct 2010		*July 2013*		
	Too far restricting civ libs	**Not far enough to protect**	**Too far restricting civ libs**	**Not far enough to protect**	**Change in % civ libs**
	%	%	%	%	
Total	32	47	47	35	+15
Men	36	45	51	29	+15
Women	29	49	42	40	+13
18-29	40	38	60	29	+20
30-49	32	45	48	36	+16
50-64	29	55	44	36	+15
65+	26	53	33	42	+7
College grad+	30	46	48	28	+18
Some college	35	44	51	32	+15
HS or less	32	50	42	42	+10

PEW RESEARCH CENTER July 17-21, 2013. Q10.

There is also a substantial gender gap: by a 51% to 29% margin men are more concerned that government policies have gone too far in restricting civil liberties. Women are divided, with 42% more worried about civil liberties and 40% more concerned that government policies haven't gone far enough to protect the country.

Modest Partisan Differences in Perceptions of Data Collection

Overall, Democrats approve of the government's data collection program by a 57%-36% margin, while Republicans (44% approve, 50% disapprove) and independents (47% approve, 48% disapprove) are more divided.

Republicans and independents also perceive the program as more far-reaching in scope and less limited. For example, 64% of Republicans and 67% of independents believe the government is collecting not only metadata but also what is being said in phone calls and emails; slightly fewer (58%) Democrats share this view.

Democrats Approve of Data Program, But Most Think Gov't Collects More than Metadata

	Total	Rep	Dem	Ind
	%	%	%	%
Gov't data collection program ...				
Approve	50	44	57	47
Disapprove	44	50	36	48
Don' know	6	6	6	4
	100	100	100	100
% who say ...				
Courts do not provide adequate limits on gov't data collection	56	59	51	59
Gov't also using data for purposes other than terrorism investigations	70	78	60	74
Gov't also collecting what is being said in calls and emails	63	64	58	67
Gov't listened or read your calls and emails	27	27	23	29

PEW RESEARCH CENTER July 17-21, 2013.
Figures may not add to 100% because of rounding.

However, these gaps in opinion are relatively modest, as half or more Democrats believe the program is not sufficiently limited by courts (51%), collects the content of communications (58%) and uses the data for purposes other than terrorism investigations (60%).

Republicans and Republican-leaning independents who agree with the Tea Party strongly disapprove of the NSA program. Overall, 62% of Tea Party Republicans disapprove of the government's data collection program, while just 34% approve. By contrast, Republicans and Republican leaners who do not agree with the Tea Party are divided in their views of the program (51% approve, 45% disapprove).

Tea Party Republicans Deeply Skeptical of NSA Program

Among Republicans and Rep-leaning independents

	Agree with Tea Party	Disagree/ No opinion
The surveillance program...	%	%
Approve	34	51
Disapprove	62	45
Don't know	4	4
	100	100

Tea Party Republicans also express far more

concern about the scope of the program. For example, fully 87% of Tea Party Republicans believe the government uses the data it collects for purposes other than terrorism investigations. When asked what other purposes the data is used for, the top answer among Tea Party Republicans – volunteered by 32% – is that the data is used to pursue political objectives or to target political opponents.

The data is...		
Used for other purposes	87	71
Only used to investigate terrorism	9	23
Don't know	4	7
	100	100
Among those who say "other purposes," percent who say the data is used to target opponents or for political ends (open-ended)	32	13

PEW RESEARCH CENTER July 17-21, 2013. Q21, Q23, Q24.

Should the Media Report on Government Anti-Terror Methods?

The public is divided over whether the news media should report on information it obtains about the secret methods the government is using to fight terrorism. About half (47%) say that the media should report on the government's secret methods, while the same percentage says they should not; overall opinion on this question is little changed from May 2006.

Both Republicans and Democrats are split on this issue – 43% of Republicans and 45% of Democrats say the media should report on secret methods to fight terrorism, while 51% of both parties say that they should not.

In 2006, there were large partisan differences on this question. At that time, Democrats thought the media should report this information by a 59%-38% margin. Most Republicans (68%) thought the news media should not report on government anti-terrorism methods, while just 26% thought that they should.

Public Divided on Media Reporting of Secret Anti-Terror Tactics

	Should media report secret methods gov't is using to fight terrorism?		
	Yes, should	**No, should not**	**DK**
	%	%	%
Total	47	47	6=100
Men	53	41	6=100
Women	41	54	5=100
College grad+	55	39	6=100
Some college	40	54	6=100
HS or less	47	48	5=100
Republican	43	51	6=100
Democrat	45	51	4=100
Independent	51	44	5=100

PEW RESEARCH CENTER July 17-21, 2013. Q27.
Figures may not add to 100% because of rounding.

Shifting Partisan Views on Reporting Secret Terror Tactics

% saying news media should report on secret methods gov't uses to fight terrorism	**May 2006**	**July 2013**	**Change**
	%	%	
Total	47	47	0
Republican	26	43	+17
Democrat	59	45	-14
Independent	53	51	-2
Rep-Dem diff	-33	-2	

PEW RESEARCH CENTER July 17-21, 2013. Q27.
2006 data from Gallup/USA TODAY.
Figures may not add to 100% because of rounding.

On Terrorism, Concerns about Both Government and Media

The public's division of opinion on whether or not the media should report the government's anti-terror methods is informed by the fact that majorities agree both with two separate statements: that the government is too secretive *and* that media reports can harm anti-terror programs.

When asked if the media reports too much information that can harm the government's anti-terrorism programs, 53% of the public agrees with this statement, while 43% disagree. At the same time, most (56%) also agree that the government keeps too much information about its anti-terrorism programs secret from the public.

Majorities Say Media Discloses Too Much, Gov't Classifies Too Much

	Agree	Dis-agree	DK
	%	%	%
Media reports too much information that can harm gov't anti-terror programs	53	43	4=100
Gov't keeps too much info about anti-terror programs secret from the public	56	39	4=100
Percent agreeing with both statements	*28*		

PEW RESEARCH CENTER July 17-21, 2013. Q58.

Comparable majorities of both Republicans and Democrats express concerns that the media reports too much information that can harm government anti-terrorism programs and that the government keeps too much information about anti-terrorism programs secret from the public.

Overall, 28% of respondents agree with both statements. Among this group slightly more (55%) say the media should not report on the government's secret anti-terrorism methods, while 41% say that they should.

Age and Views of Civil Liberties, Gov't Surveillance

As noted, young people are more likely than older people to express concern that the government's anti-terrorism policies go too far in restricting civil liberties.

Young People Concerned about Civil Liberties, Media Freedom, Divide Evenly over Surveillance

Concerns you more about government's anti-terrorism policies ...	18-29	30-49	50-64	65+	Young-old diff
	%	%	%	%	
Have gone too far in restricting civil liberties	60	48	44	33	+27
Have not gone far enough to protect the country	29	36	36	42	-13
Should media report secret					

And majorities of those under 30 (55%), as well those 30 to 49 (53%), say the news media should report on secret methods the government uses to fight terrorism. Older Americans are more opposed to the media covering secret anti-terror tactics.

Should media report secret methods government is using to fight terrorism?					
Yes, should	55	53	42	35	+20
No should not	42	43	51	56	-14
News media reports can harm anti-terror programs					
Agree	42	53	59	60	-18
Disagree	54	45	37	34	+20
Government keeps too much info about anti-terror programs secret					
Agree	64	57	56	51	+13
Disagree	33	40	40	42	-9
Government's collection of phone and internet data as part of anti-terrorism efforts					
Approve	46	49	51	51	-5
Disapprove	49	47	43	39	+10

PEW RESEARCH CENTER July 17-21, 2013. Figures read down, percent offering no opinion not shown.

Yet the large age differences about civil liberties, security and secrecy don't translate into an equally sizeable divide over the NSA surveillance program itself. About as many young people approve (46%) as disapprove (49%) of the government's data collection program. The age differences in overall opinions about the program are modest, with about half in older age groups approving of the program.

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE
Fort George G. Meade, Maryland

20 October 1980

UNITED STATES SIGNAL INTELLIGENCE DIRECTIVE (USSID)

18

LIMITATIONS AND PROCEDURES IN SIGNALS INTELLIGENCE OPERATIONS OF THE USSS (U)

LETTER OF PROMULGATION

(U) This directive 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 and privacy of U.S. persons.

(U) This USSID supersedes USSID 18, dated 26 May 1976, and is effective upon receipt.

[Signature]

B. R. INMAN
Vice Admiral, U.S. Navy
Director, NSA/Chief, CSS

CLASSIFIED BY NSA/CSSM 123-2
xxxxxxxxxxxxxxxxxxxxxxxxxx REVIEW ON 20 OCTOBER 2010

[Form]

USSID 18
20 October 1980

[Blank]

SECURITY CLASSIFICATION

CHANGE REGISTER

NO.	CHANGE DATE	AUTHORITY *(Msg Cite/DTG, Hard Copy (HC), OPSCOMM)*	ENTERED DATE	BY
1	070205Z Apr 81	(para 5.1.b(2))	9 Apr 81	xxxx
1	11 Jul 86	HC	31 Jul 86	xxxxxxx
3	20 Apr 88	xxxx 3104-88, 201128Z Apr 88	7 Jul 88	xxxx

[Balance of form blank]

FORM A 7083 REV AUG 76 *(Supercedes A 7082 Nov 72 which is obsolete)* | SECURITY CLASSIFICATION

[Blank]

20 October 1980

TABLE OF CONTENTS

[Note: Some Contents page numbers differ from directive body.]

1/ Issued Separately to Selected Recipients.

LIMITATIONS AND PROCEDURES IN SIGNALS INTELLIGENCE OPERATIONS OF THE USSS (FOUO)

SECTION 1 - REFERENCES

1.1. (FOUO) References

a. DoD Regulation 5240.1-R.

b. NSA/CSS Directive No. 10-30, dated 24 March 1980.

c. Executive Order 12036, United States Intelligence Activities, 24 January 1978.

d. 50 U S.C. 1801, Foreign Intelligence Surveillance Act of 1978, Public Law No. 95-511 (see Annex A).

SECTION 2 - PURPOSE AND APPLICABILITY

2.1. (FOUO) This USSID implements the provisions of DoD Regulation 5240.1-R for the USSS. It prescribes general policy and SIGINT operating policy, and provides procedures and assigns responsibilities to ensure that the SIGINT mission of the National Security Agency/Central Security Service is conducted in a manner that guarantees proper safeguards to the rights and privacy of U S. persons under applicable law, executive branch directives, internal directives, and policy. The annexes to USSID 18 contain procedures that must be followed for the specialized SIGINT operations and targets to which they pertain. The other policies and procedures in this USSID provide guidance in applying specific restrictions in SIGINT operations to targeting, collection, selection, storage, and dissemination of information, and the maintenance of data bases that may relate to U.S. persons. The policies and procedures herein apply to all elements of the USSS.

[Paragraph of 8 lines censored]

SECTION 3 - DEFINITIONS

3.1. (~~C~~ xxx) Agent of a foreign power, means -

a. Any person, other than a U.S person, who -
(1) 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 therefor;

(2) 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;

b. Any person, including a U.S. person, who -

(1) Knowingly engages in clandestine intelligence gathering activities for, or on behalf of, a foreign power, which activities involves, or may involve a violation of the criminal statutes of the United States;

(2) 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;

(3) Knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for, or on behalf of, a foreign power; or

(4) Knowingly aids or abets any person in the conduct of activities described in paragraphs 3.1.b. (1), 3.1.b. (2), or 3.1.b. (3) or knowingly conspires with any person to engage in such activities; or

c. A U.S. person, residing abroad, who holds an official position in a foreign government or the military forces of a foreign nation and information about whose activities in that position, would constitute foreign intelligence.

3.2. (FOUO) Available publicity 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. In this context, the "general public" also means general availability to persons in a military community even though the military community is not open to the civilian general public.

3.3. (FOUO) Clandestine intelligence activity means an activity conducted for intelligence purposes or for the purpose of affecting political or governmental processes by, or on behalf of, a foreign power in a manner designed to conceal from the United States Government the nature or fact of such activity or the role of such foreign power, and any activity conducted in support of such activity.

xxxxxxxxxxxxxxxxxxxxxxxxxxx

3.4 (~~C~~ xxx) Collection means intentional tasking and/or selection of identified nonpublic communications for subsequent processing aimed at reporting or retention as a file record.

3.5. (FOUO) Commercial organization means an organization that is not incorporated and that operates or holds itself out as a business enterprise usually, but not necessarily, for the purpose of making a profit. This term covers business pannerships, companies, associations, and sole proprietorships. Organizations that use the word "Co.," and other common commercial designations, may be treated as commercial organizations for purposes of these procedures. Some charitable, literary, and social organizations conduct incidental operations for profit, but are not thereby necessarily commercial organizations. Not every activity designed to make a profit will qualify an entity as a commercial organization. Nor will any incidental charitable, literary or social activity remove an organization from that category of commercial organization. The determination is made by assessing the predominate nature of the organization.

3.6. (FOUO) Communicant means the originator or intended recipient of a communication.

3.7. (FOUO) Communications concerning 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 reference to a product by brand name or manufacturer's name, or the use of a name in a descriptive sense, for example, "Monroe Doctrine," "Boeing 707," is not an identification of a U.S person.

3.8. (~~C~~ xxx) Consent is the 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 General Counsel, National Security Agency, to have actual or apparent authority to make such an agreement.

3.9. (FOUO) Corporation means an organization incorporated in the United States under federal, state, or local law. As regards the corporation's status as a U S. person, the fact and place of incorporation is determinative. Entirely foreign ownership does not disqualify an organization for treatment as a U.S. person under these procedures. Use of the words "Inc.," or "Corp.," in the title of an organization is sufficient for it to be treated as a corporation for purposes of these procedures.

3.10. (FOUO) Counterintelligence means information gathered and activities conducted to protect against espionage and other clandestine intelligence activities, sabotage, international terrorist activities, or assassinations conducted for, or on behalf of, foreign powers, organizations, or persons, but not including personnel, physical, document, or communications security programs.

3.11. (FOUO) Counterintelligence investigation includes inquiries and other activities undertaken to determine whether a particular U.S. person is acting for, or on behalf of, a foreign power for purposes of conducting espionage and other clandestine intelligence activities, sabotage, international terrorist activities, or assassinations and to neutralize such acts. A counterintelligence investigation, for purposes of these procedures, does not include counterespionage operations undertaken against foreign powers.

xxxxxxxxxxxxxxxxxxxxxxxxxxx

3.12. (FOUO) Electronic surveillance means acquisition of a nonpublic communication by electronic means without the consent of a person who is a party to an electronic communication or, in the case of a no electronic communication, without the consent of a person who is visibly present at the place of communication, but not including the use of radio direction finding equipment solely to determine the location of a transmitter.

3.13. (FOUO) Foreign communication means a communication that has at least one communicant outside of the United States, or that is entirely among foreign powers or between a foreign power and officials of a foreign power (but not including communications intercepted by electronic surveillance directed at premises used predominantly for residential purposes).

3.14. (FOUO) Foreign intelligence means information relating to the capabilities, intentions, and activities of foreign powers, organizations, or persons, but not including counterintelligence except for information on international terrorist activities, sabotage, and assassinations for, or on behalf of, foreign powers.

3.15. (FOUO) Foreign power means any foreign government (regardless of whether recognized by the United States), foreign-based political party (or faction thereof), foreign military force, foreign-based terrorist group, or any organization composed, in major part, of any such entity or entities. (Annex A, paragraph 2.2, defines "foreign power" for situations under the Foreign Intelligence Surveillance Act (FISA). Portions of that definition should also be used in certain situations as noted in paragraphs 6.1.b. and 8.1.e. (1).)

[3.16, 4 lines censored]

3.17. (FOUO) for the purposes of this USSID, the Intelligence Community refers to:

a. The Central Intelligence Agency;

b. The National Security Agency;

c. The Defense Intelligence Agency;

d. The offices within the Department of Defense for the collection of specialized national foreign intelligence through reconnaissance programs;

e. The Bureau of Intelligence and Research of the Department of State;

f. The intelligence elements of the military services;

g. The staff elements of the Office of the Director of Central Intelligence;

h. The intelligence elements of the Department of Treasury and the Department of Energy.

i. The intelligence elements of the Federal Bureau of Investigation (FBI); and

xxxxxxxxxxxxxxxxxxxxxxxxxxx

j. The intelligence elements of the Drug Enforcement Administration (DEA).

3.18. (FOUO) 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 not including 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.

3 19. (FOUO) International terrorist activities mean any activity or activities that:

a. Involve killing, causing serious bodily harm, kidnapping or violent destruction of property, or an attempt or credible threat to commit such acts;

b. Appear intended to endanger a protected of the Secret Service or the Department of State or to further political, social, or economic goals by intimidating or coercing a civilian population or any segment thereof, influencing the policy of a government or international organization by intimidation or coercion, or obtaining widespread publicity for a group or its cause; and

c. Transcend national boundaries in terms of the means by which it is accomplished; the civilian population, government, or international organization it appears intended to coerce or intimidate; or the locale in which its perpetrators operate or seek asylum.

3.20. (FOUO) Law enforcement means detecting violations of criminal law and identifying or apprehending persons who have violated the criminal law so that they may be prosecuted. In this context, the criminal law includes federal statutes, federal regulations, and the Uniform Code of Military Justice. *[Paragraph hand-starred in margin.]*

3.21. (FOUO) Law enforcement authorities include military police, local police, state police, the FBI, the Executive Protective Service, and special police employed by federal, state, and local government agencies. The Army Intelligence and Security Command, the Naval Investigative Service, and the Air Force Office of Special Investigations have counterintelligence responsibilities and law enforcement responsibilities under the Uniform Code of Military Justice. When engaged in law enforcement responsibilities, these components are law enforcement authorities. Components that supervise these military investigative authorities, when they are engaged in law enforcement responsibilities, are also law enforcement authorities.

3.22. (FOUO) Narcotics production or trafficking means activities outside the United States to produce or deal in narcotics or other substances controlled under the Controlled Substances Act of 1970.

3.23. (FOUO) Personnel security means the protection resulting from measures designed to ensure that persons employed in sensitive positions of trust are suitable for such employment with respect to loyalty, character, emotional stability, and reliability and that such employment is clearly consistent with the interests of the national security. It includes measures designed to ensure that persons granted access to classified information remain suitable for such access and that access is consistent with the interests of national security.

xxxxxxxxxxxxxxxxxxxxxxxxxxx

3.24. (FOUO) Physical security means the protection resulting from physical measures designed to safeguard-personnel; to prevent unauthorized access to equipment, facilities, material, and documents; and to safeguard against espionage, sabotage, damage, and theft.

3.25. (FOUO) Reasonable belief. A reasonable belief arises when the facts and circumstances are such that a reasonable person would hold the belief. Reasonable belief must rest on facts and circumstances that can be articulated; "hunches" or intuitions are not sufficient. Reasonable belief can be based on experience, training, and knowledge in foreign intelligence or counterintelligence work applied to facts and circumstances at hand, so that a trained and experienced "reasonable person" might hold a reasonable belief sufficient to satisfy this criterion when someone unfamiliar with foreign intelligence or counterintelligence work might not. Reasonable belief also depends on the circumstances in which it is formed. In emergency situations, a reasonable belief can be supported by the facts at hand and the need to take action immediately to avoid imminent harm.

3.26. (FOUO) Sabotage means any activity that involves a violation of Chapter 105 of Title 18, United States Code, or that would involve such a violation if committed against the United States.

[3.27, 4 lines censored]

[3.28, 4 lines censored]

3.29. (FOUO) Technical data base means information retained for cryptanalytic or traffic analytic purposes.

3.30. (FOUO) United States, when used to describe a place, includes the territories of the United States.

3.31. (~~C~~ xxx) U.S. person means a citizen of the United States, an alien lawfully admitted for permanent residence, an unincorporated association organized in the United States or substantially composed of United States citizens or aliens admitted for permanent residence, or a corporation incorporated in the United States.

a. The term "U.S. person" includes U.S. flag, nongovernmental aircraft or vessels. The term does not include a corporation incorporated in the United States that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments.

b. For purposes of intentionally collecting the communications of a particular person, the term "U.S. person" also includes any alien known to be presently in the United States, any group of such aliens or American citizens, any corporation, corporate subsidiary, or other legal entity having its principal place of business in the United States, and U.S. flag, nongovernmental aircraft or vessels; provided, however, that it shall not include:

(1) Any alien (other than an alien lawfully admitted for permanent residence) who, on the basis of available, reliable information, is reasonably believed to be an officer, employee, or accredited representative of a foreign power;

(2) Any group of such aliens; or

(3) Any corporation, corporate subsidiary, or other legal entity which on the basis of available, reliable information, is reasonably believed to be owned or controlled, directly or indirective by a foreign power.

c. The following guidelines will apply in determining whether a person is a U.S. person:

(1) A person known to be currently in the United States will be treated as a U.S. person unless that person is positively 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) 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 can be identified positively 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) 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 that enable such person 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.

(4) 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.

3.32. (FOUO) USSS means the unified organization for signals intelligence activities under the direction of the Director, National Security Agency/Chief, Central Security Service, comprised of the National Security Agency, the Central Security Service, the components of the military services authorized to conduct signals intelligence and such other entities (other than the FBI) as are authorized by the National Security Council or the Secretary of Defense to conduct SIGINT.

SECTION 4 - POLICY

4.1. (~~C~~ xxx) The SIGINT mission of the USSS includes the collection, processing, storage, and dissemination of foreign communications (plaintext and encrypted) passed by radio, wire, or other electromagnetic means. It is the policy of the USSS to target or collect foreign communications. The USSS will not intentionally collect the communications of U.S. persons or communications that refer to U.S. persons except as authorized pursuant to the procedures contained in this USSID or its annexes. The USSS will only process and disseminate communications of U.S. persons, or that refer to U.S. persons, as provided for in this USSID.

SECTION 5 - COLLECTION

5.1. (~~C~~ xxx) The Director, NSA, will consider requests to collect the communications of U.S. persons, or communications that refer to U.S. persons, only if one of the following criteria is satisfied:

a. The U.S. person has given consent and has executed the consent form as set forth in Annex I. Once the consent form has been executed, the Director, NSA, may authorize the collection. The Director, NSA, shall notify the Anorney General of each consensual collection.

b. The U.S. person is a foreign power or an agent of a foreign power. The purpose of the collection must be the acquisition of foreign intelligence or counterintelligence. It is also necessary that the information be unobtainable by less intrusive techniques. In this case, the Director, NSA, may:

(1) Submit an application for the collection in accordance with the FISA when the U.S. person is in the United States and the communications sought are those of that U.S. person (see Annex A).

(2) Request the Anormey General to authorize collection when the U.S. person is outside the United States, when the U.S. person is in the United States and only communications that refer to that person are sought, or when a U.S. person as defined in Section 3.31.b. is in the United States

(3) Authorize the collection if an emergency situation exists and the U.S. person is outside the United States.

5.2. (~~C~~ xxx) In emergency situations, the Director, NSA, may approve for foreign intelligence or countefintgence purposes the collection of communications of U.S. persons, or communications that refer to U.S. persons, when such persons are outside the United States and when securing the prior approval of the Attorney General is not practical.

a. An emergency situation exists when:

xxxxxxxxxxxxxxxxxxxxxxxxxxx

(1) The time required to secure Attorney General approval would cause failure or delay in obtaining significant foreign intelligence or counterintelligence and such failure or delay would result in substantial harm to the national security;

(2) Any person's life or physical safety is reasonably believed to be in immediate danger; or

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

b. The Director, NSA, shall notify the DoD General Counsel and the Attorney General as soon as possible of the nature of the collection, the circumstances surrounding its authorization, and the results thereof.

c. Such collection may not continue longer than the time required for a decision by the Attorney General and in no event longer than 72 hours.

[12 lines censored]

SECTION 6 - PROCESSING

6.1 (~~C~~ xxx) Foreign communications of, or concerning, U.S. persons must be processed in accordance with the following limitations:

[11 lines censored]

[24 lines censored]

6.3 (~~C~~ xxx) Except as approved under this USSID and its annexes, no collection may be directed that brings about the intentional interception and recording of communications solely between U.S. persons. [8 lines censored] Those non-foreign communications that may indicate threat of death or serious bodily harm to any person, or xxxxxxxxxxxxxxxxxxxxx reveal a potential vulnerability to United States Communications Security, should be forwarded to NSA/CSS,

[23 lines censored]

xxxxxxxxxxxxxxxxxxxxxxxx

SECTION 7 - STORAGE

7.1. (~~C~~ xxx) Foreign communications of, or concerning, U.S. persons that are intercepted by the USSS may be retained in their original form or as transcribed:

[16 lines censored]

b. If dissemination of such communications without elimination of references to such U.S. persons would be permitted under Section 8, below.

7.2. (FOUO) Where practicable and when recognizable, information acquired as a part of, or incidental to authorized collection activities wherein the identification of a U S. person is not necessary xxxxxxxxxxxxxxxxxxxxxxxxx for dissemination under Section 8, the U.S. person's identity shall be deleted and replaced with a generic term.

7.3. (FOUO) Storage systems shall be reasonably designed to limit access to information about U.S. persons to those with a need to know.

7.4. (FOUO) Intelligence reports based on foreign communications must be stored in accordance with the Privacy Act. Although Section 8 permits the dissemination of information containing the names of U.S. persons, such names will be deleted prior to permanent storage of intelligence reports in name retrievable files, xxxxxxxxxxxxxxx

7.5. (FOUO) Information about U.S. persons other than that covered by this section shall be stored only for purposes of reporting such collection for oversight purposes and for any subsequent proceedings that may be necessary.

SECTION 8 - DISSEMINATION

8.1. (~~C~~ xxx) Dissemination of information derived from foreign communications that includes an identification of a U.S person may be made only if one of the following criteria is met:

a. The U.S. person has consented to the use of communications of, or concerning, him or her and has executed the applicable consent form (see Annex I).

b. The information is available publicly; for example, the information is derived from unclassified collateral information available to the general public.

c. The identity of the U.S. person is necessary to understand foreign intelligence information or assess its importance; for example, the identity of a senior official in the executive Branch. Such officials, when identified, will be identified only by their official titles; for example, "President of the United States."

d. The communication or information indicates that the U.S. person may be an agent of a foreign power.

e. The communication or information that is being disseminated indicates that the U.S. person may be:

(l) A foreign power as defined in Annex A, 2.2.d and f.;

(2) Residing outside the United States and holding an official position in the government or military forces of a foreign power such that information about his activities would constitute foreign intelligence;

(3) A corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or

(4) Acting in collaboration with an intelligence or security service of a foreign power, and the U.S. person has, or has had, access to information or material classified by the United States;

f. The communication or information indicates that the U.S. person may be the target of intelligence activities of a foreign power.

g. The communication or information indicates that the U.S. 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.

h. The communication or information indicates that the U.S. person may be engaging in international terrorist activities.

i. The interception of the U.S. person's communication was authorized by a court order issued pursuant to Section 105 of the FISA and the communication may relate to the foreign intelligence purpose of the surveillance. (See Annex A.)

xxxxxxxxxxxxxxxxxxxxxxxxxx

j. The communication or information is evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes; for example, the communication or information indicates a possible threat to the life or physical safety of any person.

[25 lines censored]

8.5. (~~C~~ xxx) Any proposed report or translation based on, relating to, or relaying the contents of a privileged communication, for example, attorney-client, doctor-patient, involving a U.S. person, including for this purpose, the U S Government, must be referred xxxxxx for review prior to publication.

8.6. (FOUO) Dissemination other than that described in this section must be approved by the General Counsel to ensure compliance with applicable laws, executive orders and regulations.

SECTION 9 - RESPONSIBILITIES

9.1. (FOUO) Inspector General - The Inspector General is assigned overall staff responsibility for overseeing NSA/CSS compliance with this USSID. In carrying out this responsibility, the Inspector General:

a. Annually conducts a detailed inspection of NSA/CSS activities to ensure compliance with this USSID.

b. Reports to the Director, NSA, annually (1 October) concerning NSA/CSS compliance with this USSID.

c. Establishes procedures for reporting by Key Component and Field Chiefs of their activities and practices to the Inspector General.

d. Reports quarterly with the Director and General Counsel to the Intelligence Oversight Board through the Inspector General for Defense Intelligence.

9.2. (FOUO) The General Counsel:

a. Actively assists the Inspector General in the annual inspection of NSA/CSS activities, as required.

b. At the request of the Director, Deputy Director, Key Components Chiefs, or the Inspector General, reviews and assesses for legal implications new major requirements levied on the NSA/CSS or internal initiatives that may involve the rights of U.S. persons.

c. Reviews and obtains from the Attorney General necessary approval of new procedures.

d. Advises the Director and senior staff, NSA/CSS, of new legislation and/or case laws that may impact on NSA/CSS missions, functions, operations, activities, and practices.

e. Reports, as required, to the Intelligence Oversight Board and provides copies of such reports to the Director and affected agency elements.

[50 lines censored]

9.4. (FOUO) All Elements of the USSS:

a. Implement this directive upon receipt. Ensure adherence to the provisions of this USSID and appropriate annexes in the conduct of SIGINT operations.

b. Amend and supplement existing formal publications and informal operating instructions to conform with this USSID.

c Prepare new procedures as required to ensure adherence to this USSID. A copy of such procedures shall be forwarded to NSA/CSS, Attn: xxx

d. Immediately inform the DDO of any tasking received that appears to require actions at variance with this USSID.

SECTION 10 - ACCOUNTABILITY

[55 lines censored]

[All annexes, 28 pages]

~~SECRET~~

222

NATIONAL SECURITY AGENCY/CENTRAL SECURITY SERVICE
Fort George G. Meade, Maryland

20 October 1980

UNITED STATES SIGNAL INTELLIGENCE DIRECTIVE (USSID)

18

ANNEX A

PROCEDURES IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (U)

LETTER OF PROMULGATION

(U) This annex is issued separately for use by elements of the USSS only when conducting electronic surveillance pursuant to the Foreign Intelligence Surveillance Act (FISA). Such surveillance will be conducted only upon notification by NSA/CSS.

[Signature]

B. R. INMAN
Vice Admiral, U.S. Navy
Director, NSA/Chief, CSS

CLASSIFIED BY NSA/CSSM 123-2
xxxxxxxxxxxxxxxxxxxxxxxxxx REVIEW ON 20 OCTOBER 2010

[Form]

[Blank]

SECURITY CLASSIFICATION

CHANGE REGISTER

NO.	CHANGE DATE	AUTHORITY *(Msg Cite/DTG, Hard Copy (HC), OPSCOMM)*	ENTERED DATE	BY
[No entries]				

FORM A 7083 REV AUG 76 *(Supercedes A 7082 Nov 72 which is obsolete)* | SECURITY CLASSIFICATION

[Blank]

USSID 18
20 October 1980

ANNEX A

PROCEDURES IMPLEMENTING THE FOREIGN INTELLIGENCE SURVEILLANCE ACT (U)
INTELLIGENCE SURVEILLANCE ACT (U)

SECTION 1 - PURPOSE AND APPLICABILITY

1.1. (U) The Foreign Intelligence Surveillance Act (FISA) governs the conduct of certain electronic surveillance activities within the United States to collect foreign intelligence information. These electronic surveillance activities involve either the acquisition of wire communications by direct access in the United States, the acquisition of radio communications where all parties to that communication are located in the United States, the intentional collection of the communications of a particular, known U.S. person who is in the United States, or the acquisition of information within the United States from other than wire or radio communications.

1.2. (U) These procedures apply to the collection, processing, storage, and dissemination of communications collected by electronic surveillance authorized pursuant to FISA, Public Law 95-511 ("the Act"). The procedures also apply to the acquisition of technical intelligence, other than the spoken communications of individuals, conducted under certification of the Attorney General, pursuant to Section 102(a)(1)(A)(ii) of the Act.

SECTION 2 - DEFINITIONS

2.1. (U) In addition to the definitions in Section 3 of USSID 18, the following definitions shall apply to this annex. If a term is defined in Section 3 of USSID 18 and in this annex, only the definition in this annex shall be used for surveillance activities conducted pursuant to the Act. 2.2. (U) "Foreign power" means -

a. A foreign government or any component thereof, whether or not recognized by the United States;

b. A faction of a foreign nation, or nations, not substantially composed of U.S. persons;

c. An entity that is openly acknowledged by a foreign government or governments to be directed and controlled by such foreign government or governments;

d. A group engaged in international terrorism or activities in preparation therefor;

e. A foreign-based political organization, not substantially composed of U.S. persons; or

f. An entity that is directed and controlled by a foreign government or governments.

2.3. (U) "Foreign intelligence information means -

a. Information that relates to, and if concerning a U.S. person, is necessary to, the ability of the United States to protect against -
(1) Actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(2) Sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(3) Clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

b. Information with respect to a foreign power or foreign territory that relates to, and if concerning a U.S. person, is necessary to -

(1) The national defense or the security of the United States; or

(2) The conduct of the foreign affairs of the United States.

2.4. (U) "Contents," when used with respect to a communication, include any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication.

2.5. (U) "Electronic surveillance" means -

a. The acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by, or intended to be received by, a particular, known U.S. person who is in the United States,

if the contents are acquired by intentionally targeting that 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;

b. The acquisition by an 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 at the United States;

c. 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 for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; or

d. 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 for law enforcement purposes.

NOTE: Communication intercept activity that does not fall within the above definition and that results in the incidental acquisition of communications sent from, or intended for, receipt within the United States does not thereby become electronic surveillance within the meaning of this definition.

2.6. (U) "U.S. person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in Section 101(a)(20) of the Immigration and Nationality Act), an unincorporated association, a substantial number of members of which are citizens of the United States, or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsections 2.2a, b, or c.

2.7. (U) "Wire communication" means any communication while it is being carried by a 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.

SECTION 3 - GENERAL

3.1. (U) Collection of foreign intelligence information by electronic surveillance as defined in paragraph 2.5 shall be accomplished only in accordance with an order of the United States Foreign Intelligence Surveillance Court (USFISC) or a certification of the Attorney General. In any case in which it is necessary for the USSS to conduct electronic surveillance, a request to secure a court order or Attorney General certification will be forwarded by the appropriate Rey Component through the General Counsel to the Director. Only targets that meet the definition of either agent of a foreign power or foreign power may be considered for approval pursuant to the Act.

SECTION 4 - MINIMIZATION PROCEDURES

4.1. (U) Each surveillance authorized pursuant to the Act must be conducted pursuant to the minimization procedures approved by the USFISC or the Attorney General for that particular surveillance. Minimization procedures will be attached to each court order or Attorney General certification that is issued and will regulate the collection, processing, storage, and dissemination of information concerning unconsenting U.S. persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information.

4.2. (~~S~~) The Attorney General has approved standard minimization procedures applicable to electronic surveillance activities pursuant to the Act. These minimization procedures apply to electronic surveillances authorized by the USFISC or the Attorney General pursuant to the Act, except as provided in subsection 4.4 of this annex.

MINIMIZATION PROCEDURES

Pursuant to Section 101(h) of the Foreign Intelligence Surveillance Act of 1978, the following procedures have been adopted by the Attorney General, and shall be followed by the National Security Agency in implementing this electronic surveillance as ordered by the Court: (~~S~~)

Sec. 1 - Applicability and Scope.

[12 lines censored]

Sec. 2. Definitions.

In addition to the definitions in Section 2 of this annex, the following definitions shall apply to these procedures:

(a) Acquisition means the interception by the National Security Agency through electronic means of a communication to which it is not an intended party and the processing of the contents of that communication into an intelligible form intended for human inspection. (U)

(b) Available publicly means information that a member of the public could obtain on request, by research in public sources, or that has been obtained by casual observation. (U)

(c) Consent is the 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 General Counsel, National Security Agency, to have actual or apparent authority to make such an agreement.

(d) Identification of a United States person means the name, unique title, address or other personal identifier of a U.S. person in the context of activities conducted by that person or activities conducted by others and 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; for example, "Monroe Doctrine," is not an identification of a U.S. person. (U)

(e) Technical data base means information retained for cryptanalytic or traffic analytic purposes.

(f) U.S. person. The following guidelines will apply in determining whether a person is 2 U.S. person:

(1) A person known to be currently in the United States will be treated as a U.S. person unless that person is positively 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) 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 can be identified positively as such or the nature of the person's communications or other indicia in the contents or circumstances of such connunications give rise to a reasonable belief that such person is a U.S. person.

(3) 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 that enable such person 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.

(4) 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.

Sec. 3. Acquisition.

The collection of information by electronic surveillance subject to these procedures shall be accomplished in accordance with the certification of the Attorney General or the court order authorizing such-surveillance and will be conducted by technical means, and in a manner designed to minimize to the greatest extent reasonably feasible the acquisition of information which is not relevant to the authorized purpose of the surveillance. Collection personnel will monitor the collection of raw data at regular intervals to verify that the surveillance is not avoidably acquiring communications of U.S. persons outside the authorized scope of the surveillance or information concerning U.S. persons not related to the purpose of the surveillance. Personnel who process intercepted data into an intelligible form intended for inspection by analysts will discard inadvertently acquired communications of, or information concerning, U.S. persons at the earliest practicable point in the processing cycle at which such communication or information can be identified as clearly not relevant to the authorized purpose of the surveillance. Communications of, or information concerning, U.S. persons which may be related to the purpose of the surveillance may be forwarded to analytic personnel who are responsible for producing intelligence information from the collected data. Any such communication or information acquired a the course of an authorized surveillance may be retained and disseminated only in accordance with Sections 4 and 5 of these procedures. (~~S~~)

[12 lines censored]

[50 lines censored]

Sec. 5. Dissemination.
(a) Dissemination of intelligence reports or translations that include an identification of a U.S. person may be made only if one of the following criteria is met:
The U.S. person has consented to the use of communications of, or concerning, him or her and has executed the applicable consent form (see Annex I).

The information is available publicly; for example, the information is derived from unclassified collateral information available to the general public.

The identity of the U.S. person is necessary to understand foreign intelligence information or assess its importance; for example, the identity of a senior official.

in the Executive Branch. Such officials, when identified, will be identified only by their official titles; for example, "President of the United States."

The communication or information indicates that the U.S. person may be an agent of a foreign power.

The communication or information that is being disseminated indicates that the U.S. person may be:

A foreign power as defined in this annex, paragraph 2.2d and f;

Residing outside the United States and holding an official position in the government or solitary forces of a foreign power such that information about his activities would constitute foreign intelligence;

A corporation or other entity that is owned or controlled directly or indirectly by a foreign power; or,

Acting in collaboration with an intelligence or security service of a foreign power, and the U.S. person has, or has had, access to information or material classified by the United States;

The communication or information indicates that the U.S. person may be the target of intelligence activities of a foreign power.

The communication or information indicates that the U.S. 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.

The communication or information indicates that the U.S. person may be engaging in international terrorist activities.

The interception of the U.S. 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.

The communication or information is evidence that a crime has been, is being, or is about to be committed, provided that dissemination is for law enforcement purposes;

for example, the communication or information indicates a possible threat to the life or physical safety of any person.

(b) A report based on a communication of, or information concerning, an uncommenting U.S. person that is not publicly available may be disseminated without regard to the limitations in (a) above if the identity of the U.S. person is deleted and a generic term or symbol is substituted so that the information in the context of the communication cannot reasonably be connected with an identifiable U.S. person. (U)

(c) Reports based on the communications of, or containing information concerning, an identified uncommenting U.S. person may only be disseminated to a recipient requiring the identity of such person in the performance of official duties. (U)

(d) Upon recognition that a radio communication to which all parties are in the United States has been unintentionally acquired under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, such communication shall be destroyed promptly unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person. (U)

4.3. (~~C~~) If, during the course of electronic surveillance authorized by Attorney General certification, the contents of any communication to which a U.S. person is a party are acquired, that communication shall not be disclosed, disseminated, or used for any purpose or retained for longer than 24 hours after recognition unless a court order is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

4.4. (~~C~~) While the minimization procedures set forth in 4.2 and 4.3 are the standard procedures used for surveillance activities conducted by NSA pursuant to the Act, it may be necessary to develop special procedures on a case-by-case basis. Those procedures will be provided directly to the personnel responsible for collecting, processing, storing, and disseminating the information collected by that particular electronic surveillance.

SECTION 5 - RESPONSIBILITIES

[3 lines censored]

5.2. (U) The General Counsel will review requests to conduct electronic surveillance pursuant to the Act and will prepare applications for securing court orders and requests for Attorney General Certifications.

ANNEX B

OPERATIONAL ASSISTANCE TO THE FEDERAL BUREAU OF INVESTIGATION (U)

SECTION 1 - GENERAL

1.1. (U) In accordance with the provisions of Section 2-309(c) of E.O. 12036, the National Security Agency may provide specialized equipment and technical knowledge to the FBI to assist the Bureau in the conduct of its lawful functions. When requesting such assistance, the FBI shall certify to the General Counsel of NSA that such equipment or technical knowledge is necessary to the accomplishment of one or more of the Bureau's lawful functions.

1.2. (U) NSA may also provide expert personnel to assist Bureau personnel in the operation or installation of specialized equipment when that equipment is to be employed to collect foreign intelligence or counterintelligence. When requesting the assistance of expert personnel, the FBI shall certify to the General Counsel that such assistance is necessary to collect foreign intelligence or counterintelligence and that the approval of the Attorney General (and, when necessary. a warrant from a court of competent jurisdiction) has been obtained.

SECTION 2 - CONTROL

2.1 (U) No operational assistance as discussed in Section 1 shall be provided without the express permission of the Director, NSA/Chief, CSS.

ANNEX C

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

SECTION 1 - POLICY

1.1. (~~C~~) Signals intelligence support to U.S. and Allied military exercise command authorities is provided for in USSID 56 and DoD Directive 5200.17 (M-2). JCS Secretary's Memorandum 485-73, annexed to USSID 4, establishes 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 - DEFINITIONS

2.1. (U) Military Tactical Communications mean 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 - PROCEDURES

3.1. (~~C~~ xxx) The USSS may collect, process, store, and disseminate military tactical communications that are also communications of, or concerning, U.S persons.

a. Collection efforts will be conducted in such a manner as to avoid, to the extent feasible, the intercept of non-exercise-related communications.

b. 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. Communications of U.S. persons not participating in the exercise that are inadvertently intercepted during the exercise shall be destroyed a soon as feasible. [5 lines censored]

d. Dissemination of military exercise communications, exercise reports, or information files derived from such communications shall be limited to those authorities and persons participating in, or conducting, reviews and critiques thereof.

ANNEX D

TEST AND EVALUATION OF ELECTRONIC EQUIPMENT (U)

SECTION 1 - PURPOSE AND APPLICABILITY

1.1. (U) This annex applies to the testing (including calibration) and evaluation of electronic equipment that has the capability to intercept communications. Testing and evaluations of such electronic equipment will be conducted, to the maximum extent that is practical, without interception of the communications of U.S. persons.

SECTION 2 - PROCEDURES

2.1. (U) The USSS may test electronic equipment that has the capability to intercept communications subject to the following limitations:

a. To the maximum extent that is practical, the following should be used --
(1) Laboratory-generated signals;

(2) Department of Defense official agency communications with consent from an appropriate DoD official;

(3) Official government agency communications with consent from an appropriate official of the originating agency;

(4) Individual government employee communications with consent from the employee; or

(5) Communications transmitted between terminals located outside the United States not used by any known U.S. person.

b. Where it is not practical to test electronic equipment solely against signals described in paragraph 2.1a, above, testing may be conducted, provided –

(1) It is limited in scope and duration to that necessary to determine the capability of the equipment;

(2) No particular U.S. person is targeted intentionally without consent and it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance; and

(3) The test does not exceed 90 calendar days.

c. Where the test involves communications other than those identified in 2.1a and a test period longer than 90 days is required, a test proposal and plan shall be submitted to the Attorney General for approval. Such proposals and plans shall be submitted to the Director, NSA, through the General Counsel, NSA, 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.

2.2. (U) The content of any communication acquired during a test and evaluation shall be:

a. Retained only for the purpose of deteroining the capability of the electronic equipment;

b. Disclosed only to persons conducting or evaluating the test; and

c. Destroyed upon completion of the testing.

2.3. (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 way 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. No content of any communication may be retained or used.

ANNEX E

COMMUNICATIONS SECURITY (U)

SECTION 1 - PURPOSE

1.1. (U) This annex is provided for information purposes only since USSID are not directive for Communications Security (COMSEC) operations. Implementation of COMSEC surveillance policy and procedures is in National COMSEC Instruction (NACSI) 4000.

SECTION 2 - DEFINITIONS

2.1. (U) Communications security is the protective measures taken to deny unauthorized persons information derived from telecommunications of the U.S. Government related to the national security and to ensure the authenticity of such telecommunications. Communications security also includes the protection of communications containing government-derived unclassified information that relates to the national security. It includes the protection of telecommunications of organizations holding classified Defense contracts or otherwise involved in the industrial security program. It also includes the assessment of the vulnerability of United States communications to foreign electronic surveillance.

2.2. (U) Communications security entity means each entity subject to the guidance of the Secretary of Defense, acting as the executive agent of the United States Government, and the Director, NSA, acting for the Secretary in executing responsibilities as executive agent, that carries out any of the communications security activities of the United States Government.

2.3. (U) Hearability survey means monitoring radio communications to determine whether a particular radio signal can be received at one or more locations and, if reception is possible, to determine the quality of reception over time.

SECTION 3 - PROCEDURES

3.1. (U) Communications security monitoring may be directed against the communications of U.S. persons only:

a. With the consent of one of the parties to the communication;

b. As a part of a communication vulnerability survey (see paragraph 3.2); or

c. As part of a hearability survey.

3.2. (U) NSA may survey or authorize the survey by other communications security entities of the transmission facilities of communications common carriers, other private commercial entities, or the federal government to determine the potential vulnerability of those facilities to surveillance activities conducted by foreign powers.

a. No communication vulnerability survey may be conducted without the prior written approval of the Deputy Director for Communications Security, NSA.

b. Information collected during a communications vulnerability survey must be stored and processed as follows:

(1) No transmission may be acquired aurally.

(2) No transmission may be demultiplexed or demodulated for any purpose except to detect by a visual display device a test tone placed on the transmission by the owner or operator of the facility.

(3) No content may be acquired and no transmission may be recorded.

(4) Reports and logs may be compiled and retained, provided that no report or log may identify any person or entity except to the extent of identifying those transmission facilities that are vulnerable to surveillance by foreign powers. If the identities of the users of such facilities are not identical with the identities of the owners of the facilities, and their identities are relevant to the national security in light of the vulnerability of the facilities, the identity of such users may be obtained, provided such identities may not be obtained from the content of the transmissions themselves. The reports may be disseminated. Logs may be disseminated only if required to verify results contained in reports.

3.3. (U) NSA may conduct, or may authorize the conduct of, hearability surveys of telecommunications that are transmitted in the United States.

a. Where practicable, consent will be secured from the owner or user of the facility against which the hearability survey is to be conducted prior to the commencement of the survey.

b. Information collected during a hearability survey must be processed and stored as follows:

(1) The content of the communication may not be recorded nor included in any report.

(2) No microwave transmission may be demultiplexed or demodulated for any purpose.

(3) No report or log may identify any person or entity except to the extent of identifying the transmission facility that can be intercepted from the intercept site. If the identities of the users of such facilities are not identical with the identities of the owners of the facilities, and their identities are relevant to the purpose for which the hearability surveys has been conducted, the identity of such users may be obtained, provided such identity may not be obtained from the content of the transmission themselves.

c. Reports may be disseminated only within the United States Government. Logs may not be disseminated unless they are required to verify results contained in the reports.

USSID 18
20 October 1980

ANNEX F

SEARCH AND DEVELOPMENT OPERATIONS (U)

SECTION 1 - GENERAL

1.1. (~~C~~) This annex provides the procedures for safeguarding the rights of U.S. persons when conducting SIGINT search and development activities.

[15 lines censored]

b. 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 6 of USSID 18. *[4 lines censored]*

c. 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, provided that 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. 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 for processing and dissemination in accordance with relevant portions of USSID 18.

SECTION 2 - CONTROL

2.1. (U) The DDO shall ensure compliance with these procedures.

[Annex G censored]

USSID 18
20 October 1980

ANNEX H

TRAINING OF PERSONNEL IN THE OPERATION AHD USE OF ELECTRONIC COMMUNICATIONS AND SIGINT COLLECTION EQUIPMENT (U)

SECTION 1 - APPLICABILITY

1.1. (U) This annex applies to the training of personnel by USSS components in the operation and use of SIGINT collection equipment. This annex does not apply to the interception of communications with the consent of one of the parties to the communication.

SECTION 2 - DEFINITION

2.1. (U) Electronic communications equipment means electronic equipment capable of undetected interception of electronic or oral communications. It does not include equipment designed for use only in the transmission of communications. It does not include equipment designed to determine the direction and location of radio transmitters, such as radio direction finding equipment.

SECTION 3 - POLICY

3.1. (U) Training of USSS personnel in the operation and use of SIGINT collection equipment is conducted, to the maximum extent that is practical, without interception of the communications of U.S. persons who have not given consent.

SECTION 4 - PROCEDURES

4.1. (U) The training of USSS personnel in the operation and use of SIGINT collection equipment shall include guidance concerning the requirements and restrictions of the FISA, Executive Order 12036, and USSID 18 with respect to the unauthorized acquisition, storage, and dissemination of the content of communications of U.S. persons.

4.2. (U) The use of SIGINT collection equipment for training purposes is subject to the following limitations:

a. To the maximum extent that is practical, use of such equipment for training purposes shall be directed against intelligence targets otherwise authorized;

b. The contents of private communications of no consenting U.S. persons may not be acquired aurally unless the person is an authorized target of electronic surveillance; and

c. The electronic surveillance will be limited in extent and duration to that necessary to train personnel in the use of the equipment.

4.3. (U) The limitations in paragraph 4.2 do not apply in the following instances:

a. 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.

b. Minimal acquisition of information is permitted as required for calibration Purposes.

4.4. (U) Information collected during training that involves authorized intelligence targets may be stored in accordance with Section 7 of USSID 18 and disseminated in accordance with Section 8 of USSID 18. 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 DDO.

ANNEX I

SAMPLE CONSENT FORMS (U)

SECTION 1 - PURPOSE

1.1. (U) The consent forms, shown herein, are samples of those used to record an agreement between the U.S. person and NSA concerning the collection and dissemination of foreign communications by or about the U.S. person.

1.2. (U) The first sample form is for consent to collect and disseminate a U.S. person's communications and references to that person in foreign communications. The second sample form is for consent to collect and disseminate only references to the U.S. person in foreign communications.

[Both consent forms have large "SAMPLE" stamp across text]

FOR OFFICLAL USE ONLY

USSID 18, ANNEX I
20 October 1980

EXECUTIVE ORDER

CONSENT AGREEMENT

SIGNALS INTELLIGENCE COVERAGE

I, _____ (full name) _____, _____ (title) _____, hereby consent to the National Security Agency undertaking to seek and disseminate communications to or from or referencing me in foreign communications for the purpose of
_____.

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 Executive Order 12036 procedures, this consent covers only information that relates to the purpose stated above and is effective for the period ____(date)____ to ____(date)____.

Signals intelligence reports containing information derived from communications to or from me may only be disseminated to me and to _____. Signals intelligence reports containing information derived from communications referencing me may only be disseminated to me and to_____
except as otherwise permitted by procedures under Executive Order 12036.

(SIGNATURE)

(TITLE) (DATE)

USSID 18, ANNEX I
20 October 1980

EXECUTIVE ORDER

CONSENT AGREEMENT

SIGNALS INTELLIGENCE COVERAGE

I, _____ (full name) _____, _____ (title) _____, hereby consent to the National Security Agency undertaking to seek and disseminate references to me in foreign communications for the purpose of _____.

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 Executive Order 12036 procedures, this consent covers only references to me in foreign communications and information derived therefrom that relate to the purpose stated above. This consent is effective for the period ____ (date) ____ to ____ (date) ____.

Signals intelligence reports containing information derived from communications referencing me and related to the purpose stated above may only be disseminated to me and to _____ except as otherwise permitted by procedures under Executive Order 12036.

(SIGNATURE)

(TITLE) (DATE)

AGENCIA NACIONAL DE SEGURIDAD / SERVICIO CENTRAL DE SEGURIDAD

Fort George G. Meade, Maryland

20 de octubre 1980

DIRECTIVA DE SEÑALES DE INTELIGENCIA ESTADOS UNIDOS (USSID) 18

LIMITACIONES Y PROCEDIMIENTOS DE SEÑALES DE INTELIGENCIA OPERACIONES DE LA USSS (U)

CARTA DE PROMULGACIÓN

(U) La presente Directiva establece las políticas y procedimientos, y asigna responsabilidades para asegurar que las misiones y funciones de la TNE Estados Unidos

SIGINT System (USSS) se llevan a cabo de una manera que proteja los derechos constitucionales y de la intimidad de los ciudadanos estadounidenses.

(U) Este USSID sustituye USSID 18, de fecha 26 de mayo de 1976 y es efectivo sobre recibo.

[Firma]

B. R. INMAN

Vicealmirante, Marina de los EE.UU.

Director de la NSA / Jefe de la CSS

CLASIFICADO POR NSA / CSSM 123-2

xxxxxxxxxxxxxxxxxxxxxxxxxx REVISIÓN el 20 octubre 2010

[Form]

USSID 18

20 de octubre 1980

[Blanco]

_____

SEGURIDAD CLASIFICACIÓN

CAMBIO DE REGISTRO

_____

CAMBIO ENTRÓ

NO. AUTORIDAD DE FECHA (Msg Citar / DTG, Hard Copy (HC), OPSCOMM) FECHA DE

1 070205Z abril 81 (párrafo 5.1 b) (2) 09 de abril 81 xxxx

1 11 de julio 86 HC 31 de julio 86 xxxxxxx

3 20 de abril 88 xxxx 3104-88, 201128Z abril 88 07 de julio 88 xxxx

[Balance de formulario en blanco]

_____

FORMAR UN 7083 REV agosto 76 (Reemplaza A 7082 noviembre 72, que es obsoleto) | SEGURIDAD CLASIFICACIÓN

[Blanco]

TABLA DE CONTENIDO

[Nota: Algunos números de página Contenido difieren de órgano directivo.]

_____
1 / publicado por separado en Destinatarios seleccionados.

20 de octubre 1980

LIMITACIONES Y PROCEDIMIENTOS DE SEÑALES DE INTELIGENCIA OPERACIONES DE LA USSS (FOUO)

SECCIÓN 1 – REFERENCIAS

1.1. (FOUO) Referencias

a. Reglamento DoD 5240.1-R.

b. NSA / CSS Directiva N ° 10-30, de fecha 24 de marzo de 1980.

c. La Orden Ejecutiva 12036, United States Actividades de Inteligencia, 24 de enero de 1978.

d. 50 U SC 1801, la Ley de Vigilancia de Inteligencia Extranjera de 1978, Ley Pública No. 95-511 (véase el Anexo A).

SECCIÓN 2 - OBJETO Y CAMPO DE APLICACIÓN

2.1. (FOUO) Este USSID aplica las disposiciones del Reglamento DoD 5240.1-R para el Servicio Secreto. En él se establece la política general y la política de operación SIGINT, y proporciona los procedimientos y asigna responsabilidades para garantizar que la misión SIGINT de la Agencia / Servicio Central de Seguridad de Seguridad Nacional se lleva a cabo de una manera que garantiza las debidas garantías a los derechos y la privacidad de U S. menores legislación aplicable, las directivas del Poder Ejecutivo, las directivas internas y la política. Los anexos de USSID 18 contienen los procedimientos que deben seguirse para las operaciones SIGINT especializados y las metas a las que pertenecen. El resto de las políticas y procedimientos de este USSID proporcionan orientación en la aplicación de las restricciones específicas en las operaciones SIGINT a la focalización, la recogida, selección, almacenamiento y difusión de información y el mantenimiento de bases de datos que pueden relacionarse con personas de Estados Unidos. Las políticas y procedimientos en este documento se aplican a todos los elementos del Servicio Secreto.

[El párrafo de 8 líneas censuradas]

SECCIÓN 3 – DEFINICIONES

3.1. (C xxx) agente de una potencia extranjera, significa –

a. Cualquier persona que no sea una persona U.S, que –

(1) Los actos en los Estados Unidos como un funcionario o empleado de una potencia extranjera, o como miembro de un grupo involucrado en el terrorismo o actividades en ellos la preparación internacional;

(2) Los actos para, o en nombre de una potencia extranjera que participa en actividades clandestinas de inteligencia de los Estados Unidos contra los intereses de Estados Unidos cuando las circunstancias de la presencia de esas personas en los Estados Unidos indican que esa persona puede participar en este tipo de actividades en los Estados Unidos, o cuando dicha persona a sabiendas ayuda o incita a cualquier persona en el ejercicio de dichas actividades o, a sabiendas conspira con cualquier persona a participar en tales actividades;

b. Cualquier persona, incluyendo una persona de los EE.UU., que -

(1) se acopla a sabiendas en actividades de recolección de inteligencia clandestina para, o en nombre de una potencia extranjera, cuyas actividades implican o pueden implicar una violación de las leyes penales de los Estados Unidos;

(2) De acuerdo con la dirección de un servicio de inteligencia o de la red de una potencia extranjera, se acopla con conocimiento de causa en otras actividades clandestinas de inteligencia para, o en nombre de, como potencia extranjera, cuyas actividades implican o están a punto de implicar una violación de las leyes penales de los Estados Unidos;

(3) se acopla a sabiendas en el sabotaje o terrorismo internacional, o actividades que están en preparación para ello, por, o en nombre de una potencia extranjera, o

(4) A sabiendas ayude o instigue a cualquier persona en la realización de las actividades descritas en los párrafos 3.1.b. (1), 3.1.b. (2), o 3.1.b. (3) o con conocimiento conspira con cualquier persona a participar en la tales actividades, o

c. Una persona de los EE.UU., con domicilio en el extranjero, que tiene una posición oficial en un gobierno extranjero o de las fuerzas militares de una nación y la información sobre las actividades que en esa posición constituiría inteligencia extranjera.

3.2. (FOUO) publicidad disponible significa que la información que se ha publicado o transmitido para el consumo público en general, está disponible a petición de un miembro del público en general, se ha visto o escuchado por un observador casual, o se pone a disposición en una reunión abierta a la público en general. En este contexto, el "público en general" significa también la disponibilidad general a las personas en una comunidad militar a pesar de que la comunidad militar no está abierto al público en general civil.

3.3. (FOUO) actividad de inteligencia clandestina refiere a una actividad llevada a cabo con fines de inteligencia o con el propósito de afectar a

los procesos políticos o gubernamentales por, o en nombre de una potencia extranjera en una manera diseñada para ocultar al Gobierno de los Estados Unidos de la naturaleza o de hecho de tal actividad o el papel de dicha potencia extranjera, y cualquier actividad realizada con el apoyo de dicha actividad.

Xxxxxxxxxxxxxxxxxxxxxxxxx

3.4 (C xxx) Collecticn significa intencional selección tareas y / o de las comunicaciones no públicas identificados para su posterior procesamiento destinado a la retención de información o como un registro de archivo.

3.5. (FOUO) Organización comercial significa una organización que no se incorpora y que explota o posee a sí misma como una empresa de negocios por lo general, aunque no necesariamente, con el propósito de obtener un beneficio. Este término abarca pannerships (colaboraciones) empresariales, empresas, asociaciones y empresas individuales. Las organizaciones que utilizan la palabra "Co.", y otras denominaciones comerciales comunes, pueden ser tratadas como organizaciones comerciales a los efectos de estos procedimientos. Algunas organizaciones de caridad, literarias y sociales realizan estas operaciones casuales pero no son organizaciones con ello necesariamente comerciales. No todas las actividades destinadas a obtener un beneficio tendrá derecho a una entidad como una organización comercial. Tampoco ninguna actividad incidental caritativa, literarias, sociales o eliminar una organización de ese tipo de organización comercial. La determinación se realiza mediante la evaluación de la naturaleza predominante de la organización.

3.6. (FOUO) comulgante, el ordenante o destinatario de una comunicación.

3.7. (FOUO) Comunicaciones relativas a una persona de EE.UU. son aquellos en los que la persona EE.UU. se identifica en la comunicación. Una persona EE.UU. se identifica cuando el nombre de la persona, único título, dirección, u otra identificación personal se revela en la comunicación en el contexto de las actividades realizadas por la persona o las actividades realizadas por los demás y en relación con esa persona. Una referencia a un producto, marca o nombre del fabricante, o el uso de un nombre en un sentido descriptivo, por ejemplo, "Doctrina Monroe", "Boeing 707", no es una identificación de una persona de los EE.UU.

3.8. (C xxx) El consentimiento es el acuerdo por una persona u organización para permitir que los USSS tomar acciones concretas que afectan a la persona u organización. Un acuerdo por una organización con la Agencia de Seguridad Nacional que permita la recogida de información se considerará como consentimiento válido si se le da el nombre de dicha organización por un funcionario u órgano de gobierno, decidido por el Consejo General de la Agencia de Seguridad Nacional, que tiene autoridad real o aparente para que dicho acuerdo.

3.9. (FOUO) Corporación se entiende una organización constituida en los Estados Unidos bajo las leyes federales, estatales o locales. En cuanto a la situación de la empresa como una persona U.S. el hecho y lugar de incorporación es determinante. Propiedad totalmente extranjera no descalifica a una organización para el tratamiento como una persona de los EE.UU. en virtud de estos procedimientos. El uso de las palabras "Inc.", o "Corp.", en el título de una organización es suficiente para que sea tratada como una corporación con fines de estos procedimientos.

3.10. (FOUO) Contrainteligencia es la información recopilada y las actividades llevadas a cabo para proteger contra el espionaje y otras actividades clandestinas de inteligencia, sabotaje, actividades terroristas internacionales, o los asesinatos llevados a cabo por, o en nombre de, los poderes extranjeros, organizaciones o personas, pero sin

incluir el personal, físico , documento o los programas de seguridad de comunicaciones.

3.11. (FOUO) investigación de contrainteligencia incluye investigaciones y otras actividades llevadas a cabo para determine si una persona en particular EE.UU. actúa para o en nombre de una potencia extranjera a los efectos de la realización de espionaje y otras actividades clandestinas de inteligencia, sabotaje, actividades terroristas internacionales, o los asesinatos y para neutralizar tales actos. Una investigación de contrainteligencia, a los efectos de estos procedimientos, no incluye las operaciones de contraespionaje emprendidas contra las potencias extranjeras.

xxxxxxxxxxxxxxxxxxxxxxxxx

3.12. (FOUO) La vigilancia electrónica significa la adquisición de una comunicación pública por medios electrónicos sin el consentimiento de una persona que es parte de una comunicación electrónica o, en el caso de una comunicación no electrónica, sin el consentimiento de una persona que está visiblemente presente en la lugar de la comunicación, pero no incluyendo el uso de equipos de radiogoniometría únicamente para determinar la ubicación de un transmisor.

3.13. (FOUO) Comunicación Exterior, una comunicación que tenga por lo menos un comulgante fuera de los Estados Unidos, o que es enteramente entre las potencias extranjeras o entre una potencia extranjera y funcionarios de una potencia extranjera (excepto las comunicaciones interceptadas por la vigilancia electrónica dirigidos a los locales utilizado principalmente para fines residenciales).

3.14. (FOUO) Inteligencia Extranjera significa información relacionada con las capacidades, intenciones y actividades de las potencias extranjeras, organizaciones o personas, pero sin incluir la contrainteligencia excepción de la información sobre las actividades internacionales de terrorismo, sabotaje y asesinatos por, o en nombre de las potencias extranjeras.

3.15. (FOUO) Potencia extranjera significa que cualquier gobierno extranjero (independientemente de que sea reconocido por los Estados Unidos), partido político extranjero con sede en (o fracción del mismo), la fuerza militar extranjera, un grupo terrorista con sede extranjera, o cualquier organización compuesta, en su mayor parte, de cualquier entidad o entidades. (Anexo A, punto 2.2, se define la "potencia extranjera" para situaciones de conformidad con la Ley de Vigilancia de Inteligencia Extranjera (FISA). Algunas partes de esta definición también se debe utilizar en ciertas situaciones como se ha señalado en los apartados 6.1.b. y 8.1.e. (1).)

[3.16, 4 líneas censuradas]

3.17. (FOUO) A los efectos del presente USSID, la comunidad de inteligencia se refiere a:

a. La Agencia Central de Inteligencia;

b. La Agencia Nacional de Seguridad;

c. La Agencia de Inteligencia de la Defensa;

d. Las oficinas del Departamento de Defensa para la recopilación de inteligencia exterior nacional especializada a través de los programas de reconocimiento;

e. La Oficina de Inteligencia e Investigación del Departamento de Estado;

f. Los elementos de los servicios de inteligencia militar;

g. Los elementos del personal de la Oficina del Director de Inteligencia Central;

h. Los elementos de inteligencia del Departamento del Tesoro y el Departamento de Energía.

i. Los elementos de inteligencia del Buró Federal de Investigaciones (FBI), y

xxxxxxxxxxxxxxxxxxxxxxxx

j. Los elementos de inteligencia de la Agencia Antidrogas (DEA).

3.18. (FOUO) Interceptación significa la adquisición por los USSS través de medios electrónicos de comunicación pública en el que no es un partido previsto, así como el tratamiento de los contenidos de esta comunicación en forma inteligible, pero sin incluir la visualización de las señales en la pantalla visual dispositivos destinados a permitir el examen de las características técnicas de las señales sin hacer referencia al contenido de información transportado por la señal.

3 19. (FOUO) actividades terroristas internacionales significan cualquier actividad o actividades que:
a. Implicar matar, causar daños corporales graves, secuestro o destrucción violenta de la propiedad, o un intento o amenaza verosímil de cometer tales actos;

b. Aparece la intención de poner en peligro a un protegido del servicio secreto o el Departamento de Estado o de objetivos además políticos, sociales o económicos de intimidar o coaccionar a la población civil o cualquier segmento de la misma, que influyen en la política de un gobierno u organización internacional mediante la intimidación o la coerción, o la obtención de una amplia publicidad para un grupo o su causa, y

c. Trascienden las fronteras nacionales, en términos de los medios por los que se lleva a cabo, a la población civil, el gobierno o una organización internacional parece destinado a coaccionar o intimidar, o la localidad en la que sus autores operan o buscan asilo.

3.20. (FOUO) Aplicación de la ley significa detectar violaciones del derecho penal y la identificación o aprehensión de personas que han violado la ley penal para que puedan ser procesados.En este contexto, la ley penal incluye los estatutos federales, los reglamentos federales y el Código Uniforme de Justicia Militar. [Párrafo mano protagonizado margen.]

3.21. (FOUO) Las autoridades policiales son la policía militar, policía local, la policía estatal, el FBI, el Servicio de Protección Ejecutiva y la policía especial empleados federales, estatales y del gobierno local. La Inteligencia del Ejército y el Comando de Seguridad, el Servicio de Investigación Naval y la Fuerza Aérea Oficina de Investigaciones Especiales tienen responsabilidades de contrainteligencia y responsabilidades policiales bajo el Código Uniforme de Justicia Militar. Cuando participan en las responsabilidades de la ley, estos componentes son los cuerpos de seguridad. Los componentes que supervisan estas autoridades de investigación militar, cuando se dedican a la Administración de Justicia, son también las fuerzas del orden.

3.22. (FOUO) la producción o el tráfico de estupefacientes se entiende las actividades fuera de los Estados Unidos para producir o tratar de estupefacientes u otras sustancias controladas en virtud de la Ley de Sustancias Controladas de 1970.

3.23. (FOUO) El personal de seguridad se entiende la protección resultante de las medidas destinadas a garantizar que las personas que trabajan en posiciones sensibles de confianza son adecuados para este tipo de empleo con respecto a la lealtad, el carácter, la estabilidad emocional, y la fiabilidad, y que este tipo de empleo es claramente

compatible con los intereses de la seguridad nacional. Incluye medidas destinadas a garantizar que las personas acceso a la información clasificada se mantienen adecuadas para tal acceso y que el acceso sea compatible con los intereses de la seguridad nacional.

Xxxxxxxxxxxxxxxxxxxxxxxx

3.24. (FOUO) La seguridad física se entiende la protección resultante de las medidas físicas destinadas a salvaguardar-personal, para evitar el acceso no autorizado a los equipos, instalaciones, materiales y documentos, y para proteger contra el espionaje, el sabotaje, daños y robo.

3.25. (FOUO) Creencia razonable. Una creencia razonable surge cuando los hechos y las circunstancias son tales que una persona razonable sostener la creencia. Creencia razonable debe basarse en hechos y circunstancias que pueden ser articuladas, "corazonadas" o intuiciones no son suficientes. Creencia razonable puede basarse en la experiencia, la formación y el conocimiento de la inteligencia extranjera o contrainteligencia trabajo aplicado a los hechos y circunstancias a la mano, por lo que una "persona razonable" capacitado y con experiencia podría tener una creencia razonable suficiente para satisfacer este criterio cuando alguien no familiarizado con inteligencia o contrainteligencia obra extranjera no. Creencia razonable también depende de las circunstancias en las que se forma. En situaciones de emergencia, una creencia razonable puede ser apoyada por los hechos en cuestión y la necesidad de tomar medidas de inmediato para evitar un daño inminente.

3.26. (FOUO) Sabotaje, cualquier actividad que suponga una violación del Capítulo 105 del Título 18, Código de Estados Unidos, o que implicaría una violación si se cometen contra los Estados Unidos.

[3.27, 4 líneas censuradas]

[3.28, 4 líneas censuradas]

3.29. (FOUO) Técnica de base de datos significa que la información retenida para fines criptoanalíticos o el tráfico analítico.

3.30. (FOUO) Estados Unidos, cuando se utiliza para describir un lugar, incluye los territorios de los Estados Unidos.

3.31. (C xxx) Persona de EE.UU. significa un ciudadano de los Estados Unidos, un extranjero legalmente admitido para residencia permanente, una asociación no incorporada organizado en los Estados Unidos o compuesta sustancialmente por ciudadanos de los Estados Unidos o extranjeros admitidos como residentes permanentes, o de una sociedad constituida en el Estados Unidos.

a. El término "persona de los EE.UU." incluye bandera de los EE.UU., aviones o buques gubernamentales. El término no incluye a una sociedad constituida en los Estados Unidos que se reconoció abiertamente por un gobierno extranjero o de los gobiernos para ser dirigido y controlado por dicho gobierno o gobiernos extranjeros.

b. Para efectos de la percepción intencional de las comunicaciones de una persona en particular, el término "persona de los EE.UU." también incluye cualquier extranjero que se sabe que en la actualidad en los Estados Unidos, un grupo de esos extranjeros o ciudadanos estadounidenses, cualquier corporación, empresa filial, u otra entidad legal que tiene su centro de actividad principal en los Estados Unidos, y la bandera de EE.UU., las aeronaves o los buques no gubernamental, siempre que, sin embargo, que no incluirá:

(1) Cualquier extranjero (que no sea un extranjero legalmente admitido para residencia permanente) que, sobre la base de información fiable disponible, se cree razonablemente que sea un funcionario, empleado o representante acreditado de una potencia extranjera;

(2) Cualquier grupo de esos extranjeros, o

(3) Cualquier corporación, subsidiaria de la empresa o cualquier otra entidad jurídica sobre la base de información fiable disponible, se cree razonablemente que sea propiedad o esté controlada directa o indirecta por una potencia extranjera.

c. Las siguientes directrices se aplicarán para determinar si una persona es una persona de los EE.UU.:

(1) Una persona se sabe que son actualmente en los Estados Unidos va a ser tratado como una persona de los EE.UU. a menos que la persona se identifica positivamente como un extranjero que no ha sido admitido para residencia permanente o si la naturaleza de las comunicaciones de la persona u otros indicios del contenido o circunstancias de este tipo de comunicaciones dan lugar a una creencia razonable de que dicha persona no es una persona de los EE.UU.

(2) Una persona que se sabe que son actualmente fuera de los Estados Unidos, o cuya ubicación no se conoce, no se trata como una persona de los EE.UU. a menos que dicha persona puede ser identificado positivamente como tales o de la naturaleza de las comunicaciones de la persona u otros indicios del contenido o circunstancias de este tipo de comunicaciones dan lugar a una creencia razonable de que dichas personas sean U. S. persona.

(3) Una persona que sabe que es un extranjero admitido para residencia permanente se puede suponer que ha estado perdido como persona de los EE.UU. si la persona sale de los Estados Unidos y se sabe que la persona no está de acuerdo con los trámites administrativos previstos en la ley que permita a dicha persona a reingresar a los Estados Unidos sin tener en cuenta las disposiciones de la ley que otra manera, restringe la entrada de un extranjero en los Estados Unidos. El no seguir los procedimientos legales constituye una base razonable para concluir que tal extranjero ha abandonado toda intención de mantener la condición de residente permanente.

(4) Una asociación sin personería jurídica cuya sede se encuentra fuera de los Estados Unidos puede presumir de no ser una persona de EE.UU. a menos que el Servicio Secreto dispone de información que indique que un número importante de sus miembros son ciudadanos de los Estados Unidos o extranjeros legalmente admitidos para residencia permanente.

3.32. (FOUO) Servicio Secreto significa que la organización unificada para señales de actividades de inteligencia, bajo la dirección del Director del Servicio de Seguridad Nacional, la Agencia / Jefe de la Central de Seguridad, integrado por la Agencia de Seguridad Nacional, el Servicio Central de Seguridad, los componentes de los servicios militares autorizados para llevar a cabo señales de inteligencia y toda otra entidad (que no sea el FBI) que sean autorizadas por el Consejo Nacional de Seguridad o del Secretario de Defensa para llevar a cabo SIGINT.

SECRET

USSID 18
20 de octubre 1980

SECCIÓN 4 - POLÍTICA

4.1. (C xxx) La misión SIGINT del Servicio Secreto incluye la recolección, procesamiento, almacenamiento y difusión de comunicaciones extranjeras (texto claro y cifrado) aprobadas por radio, cable u otros medios electromagnéticos. Es la política del Servicio Secreto para atacar o recaudar comunicaciones extranjeras. El Servicio Secreto no recopilará deliberadamente las comunicaciones de personas o de comunicación de Estados Unidos que se refieren a personas de Estados Unidos excepto conforme a lo autorizado a los procedimientos contenidos en este USSID o sus anexos. El Servicio Secreto sólo elaborar y difunde las comunicaciones de personas de Estados Unidos, o que hacen referencia a personas de Estados Unidos, según lo dispuesto en la presente USSID.

SECCIÓN 5 - RECOPILACIÓN

5.1. (C xxx) El Director de la NSA, examinará las solicitudes para recoger las comunicaciones de personas de Estados Unidos, o las comunicaciones que se refieren a personas de Estados Unidos, sólo si uno de los siguientes criterios se cumple:

a. La persona EE.UU. ha dado su consentimiento y se ha ejecutado el formulario de consentimiento como se establece en el anexo I. Una vez que el formulario de consentimiento ha sido ejecutado, el Director de la NSA, podrán autorizar la recogida. El Director de la NSA, notificará al Procurador General de cada colección consensual.

b. La persona EE.UU. es una potencia extranjera o un agente de una potencia extranjera. El propósito de la colección debe ser la adquisición de inteligencia o contrainteligencia extranjera. También es necesario que la información sea imposible de obtener mediante técnicas menos invasivas. En este caso, el Director de la NSA, podrá:

(1) Presentar una solicitud para el cobro de acuerdo con la FISA cuando la persona en los EE.UU. está en los Estados Unidos y las comunicaciones solicitadas son las de esa persona EE.UU. (véase el Anexo A).

(2) Solicitar a la anomia General que autorice la colección cuando la persona en los EE.UU. está fuera de los Estados Unidos, cuando la persona en los EE.UU. está en los Estados Unidos y se buscan sólo las comunicaciones que se refieren a esa persona, o cuando una persona EE.UU. tal como se define en la Sección 3.31 . b. está en los Estados Unidos

(3) Autorizar la colección si existe una situación de emergencia y la persona que EE.UU. está fuera de los Estados Unidos.

5.2. (C xxx) En situaciones de emergencia, el Director de la NSA, pueda aprobar para fines de inteligencia o countefintmgence extranjeros la colección de las comunicaciones de personas de Estados Unidos, o las

comunicaciones que se refieren a personas de Estados Unidos, cuando esas personas están fuera de los Estados Unidos y al fijar el previo aprobación del Fiscal general no es práctico.

a. Una situación de emergencia se produce cuando:

xxxxxxxxxxxxxxxxxxxxxxxx

(1) El tiempo necesario para asegurar la aprobación Procurador General causar una falla o demora en la obtención de inteligencia extranjera significativa o contrainteligencia y dicho incumplimiento o retraso supondría un perjuicio sustancial para la seguridad nacional;

(2) la vida de cualquier persona física o seguridad se cree razonablemente que sea un peligro inmediato, o

(3) La seguridad física de una instalación de defensa o de propiedad del gobierno se cree razonablemente que sea un peligro inmediato.

b. El Director de la NSA, lo notificará al Consejo General del Departamento de Defensa y el Fiscal General lo antes posible a la naturaleza de la colección, la circunstancia que rodea su autorización, y los resultados de los mismos.

c. Esta colección no puede seguir más tiempo que el requerido para que una decisión de la Fiscalía General y en ningún caso más de 72 horas.
[12 líneas censuradas]

SECCIÓN 6 - TRATAMIENTO

6.1 (C xxx) Comunicaciones Exteriores de, o en relación, a los ciudadanos estadounidenses deben ser procesados de acuerdo con las siguientes limitaciones:

[11 líneas censuradas]

xxxxxxxxxxxxxxxxxxxxxxxxx

[24 líneas censuradas]

6.3 (C xxx) A excepción de lo autorizado en virtud de este USSID y sus anexos, no puede dirigirse colección que trae la interceptación intencional y la grabación de las comunicaciones exclusivamente entre personas estadounidenses. [8] Estas líneas censuradas comunicaciones no extranjeros que pueden indicar una amenaza de muerte o grave daño corporal a cualquier persona, o xxxxxxxxxxxxxxxxxxxxxx revelan una vulnerabilidad potencial de Estados Unidos Comunicaciones Security, deberán enviarse a la NSA / CSS,

[23 líneas censuradas]

xxxxxxxxxxxxxxxxxxxxxxxx

SECCIÓN 7 - ALMACENAMIENTO

7.1. (C xxx) Comunicaciones Exteriores de, o en relación, a los ciudadanos estadounidenses que son interceptados por los USSS pueden ser retenidos en su forma original o como transcrito:
[16 líneas censuradas]

b. Cuando la difusión de este tipo de comunicaciones sin la eliminación de las referencias a esas personas de Estados Unidos estaría permitido bajo la Sección 8, a continuación.

7.2. (FOUO) Siempre que sea posible y cuando reconocible, la información adquirida como parte de, o incidentales a las actividades de recogida autorizados en los que la identificación de una persona S. U no es xxxxxxxxxxxxxxxxxxxxxxxxx necesaria para su difusión en la sección 8, la identidad de la persona EE.UU. se suprimirá y se sustituirá con un término genérico.

7.3. (FOUO) Los sistemas de almacenamiento deben estar diseñados razonablemente para limitar el acceso a la información sobre los ciudadanos estadounidenses a los que tienen la necesidad de saber.

7.4. (FOUO) Los informes de inteligencia basados en comunicaciones extranjeras deben ser almacenados de acuerdo con la Ley de Privacidad. Aunque la Sección 8 permite la difusión de información que contenga los nombres de personas de Estados Unidos, estos nombres se eliminarán antes del almacenamiento permanente de los informes de inteligencia en nombre de los archivos recuperables, xxxxxxxxxxxxxxx

7.5. (FOUO) Información sobre las personas de Estados Unidos que no sean los contemplados en esta sección se almacena sólo a los efectos de la transmisión de dicha colección para fines de supervisión y de cualquier otro procedimiento ulterior que pueda ser necesaria.

xxxxxxxxxxxxxxxxxxxxxxxxx