



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

FOIA Case: 100386F  
21 September 2018

SCARLET KIM  
PRIVACY INTERNATIONAL  
62 BRITTON STREET  
LONDON EC1M 5UY  
GBR

Dear Ms. Kim:

This further responds to your Freedom of Information Act (FOIA) request of 13 December 2016 for "access to records relating to the British-United States Communication Intelligence Agreement (now known as the "UKUSA Agreement")." There are no assessable fees for this request.

This is our sixth and final production in this case. Your request has been processed under the FOIA and 16 responsive documents are enclosed. The documents total 167 pages and are annotated as NSA FOIA Case 100386 pages 00430 - 00596. Certain information, however, has been deleted from the enclosures and 5 documents (55 pages) have been withheld in their entirety.

The withheld information has been found to be currently and properly classified in accordance with Executive Order (E.O.) 13526. The information meets the criteria for classification as set forth in Subparagraphs (b) for foreign government information, (c) for intelligence activities, intelligence sources or methods, or cryptology, and/or (d) for foreign relations or activities of the U.S., of Section 1.4 and remains classified up to the TOP SECRET level as provided in Section 1.2 of E.O. 13526. The information is classified because its disclosure could reasonably be expected to cause exceptionally grave damage to the national security and because of potential harm to our foreign relationships. Because the information is currently and properly classified, it is exempt from disclosure pursuant to the first exemption of the FOIA (5 U.S.C. Section 552(b)(1)).

In addition, this Agency is authorized by various statutes to protect certain information concerning its activities. We have determined that such information exists in these documents. Accordingly, those portions are exempt from disclosure pursuant to the third exemption of the FOIA, which provides for the withholding of information specifically protected from disclosure by

FOIA Case: 100386F

statute. The specific statutes applicable in this case are Title 18 U.S. Code 798; Title 50 U.S. Code 3024(i); and Section 6, Public Law 86-36 (50 U.S. Code 3605).

Sincerely,

  
*for*

JOHN R. CHAPMAN  
Chief, FOIA/PA Office  
NSA Initial Denial Authority

Encls:

a/s

## STRATEGY FOR MAXIMIZING THE CONTRIBUTIONS OF SECOND PARTIES

### 1. Statement of Task

~~(S-CCO)~~ To develop a strategy that will lead to revised and more productive SIGINT relationships with Second Party SIGINT centers and secure an Agency commitment to manage these relationships. The strategy seeks to focus the collective efforts of the U.S. and Second Party SIGINT Systems on tasks deemed to be high priority SIGINT targets, to reduce areas of unnecessary redundancy, and to eliminate projects of marginal value thus providing for a more efficient and productive Second Party relationship. This strategy is predicated on the Second Party Principles previously approved by the Board of Directors and employs the concept of joint goals and objectives.

### 2. Basis for Strategy

A. ~~(S-CCO)~~ Predictions for the future of the SIGINT system indicate that we are facing an increasingly complex and sophisticated target environment. These trends, the ready availability of state-of-the-art technology to Soviet Bloc, Western and non-aligned nations alike, together with increased demands for intelligence, coupled with resource constraints, are forcing us to reevaluate current operations and priorities and to make difficult decisions about resource allocation and new directions.

B. ~~(S-CCO-NP)~~ Combined U.S. and Second Party resources have the potential for meeting these challenges if all parties commit to efforts that build on their unique capabilities, e.g., geography, resources, specialized skills, advanced technology, etc., and move aggressively toward achieving operational parity within the relationship, as their respective economies permit.

### 3. The Strategy

A. ~~(S-CCO-NP)~~ The strategy is based in large part on the Third Party Management Program which is working well and was developed to address many of the same kinds of problems we face in dealing with Second Parties. It comprises Country Plans, an NSA Steering Group, and Joint Goals and Objectives.

#### B. Country Plans

~~(S-CCO-NP)~~ A key part of this strategy is the development of a consolidated Agency position for each Second Party. To provide a basis for formulating this position, a plan for each Second Party will be drafted based upon the Second Party principles and current interaction with each center. These plans will be similar in intent to the plans developed for Third Parties but will be more comprehensive in nature. They will include:

Approved for Release by NSA on 09-20-2018,  
FOIA Litigation Case #100386

~~Classified by NSA/CSSM 123-2~~  
~~Declassify on: Originating Agency's Determination Required~~

**NOFORN**

~~SECRET~~

1. A review of the current status of the relationship with the Second Party center.

2. The generic set of tasks NSA would have the Second Party undertake, and the SIGINT capabilities we will encourage the Second Party to develop (i.e., where we want to go).

An important consideration in constructing these plans will be our assessment of the Second Party's capability and potential to assume greater responsibility for SIGINT "packages," (i.e., to perform all tasks for a given target from collection through reporting). Plans will be intended for use down to the NSA middle management level and will be distributed accordingly.

#### C. NSA Steering Group

~~(S-CCO-NF)~~ Following the drafting of plans for each Second Party, an NSA Second Party Steering Group chaired by DDPP and composed of NSA Senior Managers, will review and approve the plans and formulate objectives which will serve as the basis for all SIGINT negotiations and planning with the Second Party over the immediate ten to twelve months. Meetings of the Steering Group should be planned to coincide with preparation for bilateral or multilateral Second Party conferences in order to confirm or modify the Agency position on issues and actions vis-a-vis each Second Party center.

#### D. Joint Goals and Objectives

~~(S-CCO-NF)~~ Also as part of our strategy DDPP, after Country Plans have been approved, will undertake bilateral negotiations to establish a set of joint goals and objectives with DSD, CSE, and GCSB, as we have already done with GCHQ. The agreement on joint goals and objectives will help ensure that the Second Parties will direct their efforts and commit resources to mutually beneficial endeavors. In this way, the joint goals and objectives will be a means of strengthening our relationships with each of the other centers. They will also be used to measure the progress of collective operations and overall system performance.

E. ~~(S-CCO-NF)~~ Second Party efforts in meeting and resolving NSA objectives will have a direct bearing on future levels of USSS cooperation with those parties. NSA management must be prepared to address circumstances in which a Second Party center cannot or will not cooperate in a current or proposed operation. Our response should be firm, pragmatic, appropriate and formulated in a manner to promote cooperation.

#### 4. Responsibilities

##### A. DDPP

~~(S-CCO-NF)~~ The DDPP, as Steering Group Chairman and the

~~SECRET~~

~~Agency focal point for all Second Party planning and policy, will:~~

1. Convene Steering Group meetings at least semi-annually;
2. Task the Directorate of Plans, Policy and Foreign Relations with the development and updating of Second Party plans, and joint goals and objectives; and
3. Negotiate joint goals and objectives with CSE, DSD, and GCSB and monitor implementation of these joint goals and objectives.

B. DDO

~~(S-CCO-NF)~~ The DDO will be responsible for:

1. Providing input to and direction for the Country Plans; and
2. Implementing those actions (peculiar to the Operations Directorate) agreed upon by the NSA Second Party Steering Group.

C. DDT, DDR

~~(S-CCO-NF)~~ DDR and DDT will be responsible for implementing the actions agreed upon by the Second Party Steering Group within their Directorates. Specifically, they will:

1. Appoint appropriate coordinators, project managers, etc., as necessary, to carry out agreed upon Second Party actions in conjunction with DDO appointed working groups and coordinators;
2. Provide technical advice and support during the development and implementation of Second Party plans and programs; and
3. Identify areas where Second Party centers have technical expertise or capabilities that the USSS should take advantage of.

5. Recommendations

A. ~~(S-CCO)~~ That the Director, NSA, establish a Senior Management Steering Group composed of the DDO, DDT, DDPP, and DDR, and chaired by the DDPP, to provide guidance and direction in Second Party relations. Chief O3 will serve as Executive Secretary.

B. ~~(S-CCO-NF)~~ That this Steering Group meet at least semi-annually to review country plans and our relations with Second

~~SECRET~~

~~Parties, and set objectives for Second party development and activities.~~ Meetings should be scheduled to coincide with planning for major conferences and meetings with senior-level Second Party managers.

C. That the DDO, DDR, and DDT appoint senior level Second Party coordinators to effect their respective roles in the Second Party Strategy.

D. ~~(S-CCO-NF)~~ That Chiefs of O1 and O3 be directed to develop draft plans for each of the Second Party centers based upon the information provided by Key Components. These drafts are to be delivered to the Steering Group for its consideration, modification, and approval.

E. ~~(S-CCO-NF)~~ Following the approval of the CSE, DSD, and GCSB country plans, that DDPP draft joint goals and objectives for each of these Second Parties. Upon receipt of Steering Group approval, the DDPP will coordinate these joint goals and objectives with each of the Second Party centers.

~~NOFORN~~

②

DDP \_\_\_\_\_  
 DDG \_\_\_\_\_  
 DDH \_\_\_\_\_  
 DDI \_\_\_\_\_  
 DDO \_\_\_\_\_  
 DDP \_\_\_\_\_  
 DDS \_\_\_\_\_  
 DDT \_\_\_\_\_  
 EA \_\_\_\_\_  
 MS \_\_\_\_\_  
 CC: NIS  
 NSR

EXECUTIVE DIRECTOR

JMS

To: DIR  
 DDIR  
 DBI  
 DDO  
 DDP  
 DDS  
 DDT

Subject: UKUSA Relationship

[redacted] has provided the attached paper.  
 I believe this should be another input for your  
 discussions at the pre-IMR offsite.

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

[Large redacted area]

[Small redacted box]

19-17-2-93



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

<u>FROM:</u> <div style="border: 1px solid black; width: 100px; height: 30px; margin: 5px;"></div>	<u>DTG:</u> 261110Z Apr 93
<u>TO:</u> Mr. Parsons Exec DIR	<u>NUMBER OF PAGES</u> <u>(INCLUDING COVER SHEET)</u> 11
<u>CLASSIFICATION:</u> <del>TS-CEO</del> <del>NOFORN</del>	<u>TIME OF RECEIPT:</u>
<u>PASSING INSTRUCTIONS:</u>	



~~TOP SECRET~~  
Special U.S. Liaison Officer, London

26 April 1993

TO: EXEC DIR

Don,

Attached is the paper on the UKUSA relationship that I mentioned to you was being written.

I would appreciate you reading it and giving me your views and then distribute it as you see fit.

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

[Redacted]

[Redacted]

Encl:  
a/s

Classified By NSA/CSSM 123-2  
Declassify On: Originating Agency's Determination Required

~~TOP SECRET~~ ~~NOFORN~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET NOFORN~~

UNITED STATES GOVERNMENT

# memorandum

DATE: 23 April 1993

Serial: SUSL0L-011-93

REPLY TO  
ATTN OF: SUSL0L

SUBJECT: UKUSA SIGINT Relationship

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

TO: DISTRIBUTION

~~THIS MEMO IS CLASSIFIED TOP SECRET-HANDLE VIA COMINT CHANNELS ONLY-NOT RELEASABLE TO FOREIGN NATIONALS IN ITS ENTIRETY.~~

1. Attached is a paper that attempts to provide a current perspective of the UKUSA SIGINT relationship. It is a follow-up to our 15 July 1991 paper on the Implications for UKUSA of [redacted] however, updated based on more recent developments resulting from the collapse of communism in Europe and the affect that event is having in the UK, Europe, and the United States as it concerns the UKUSA relationship.

2. This paper does not make a case for drastic alteration of the present relationship as that is neither possible nor desirable. However, it does suggest that we need to give it the attention that it's importance suggests [redacted]

[redacted] As these developments continue to unfold, we will continue to provide our views.

3. I apologize for the length of the paper, but it is a complex subject with many facets and we have erred on the side of excess rather than risk failing to make the necessary points.

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

Special United States Liaison Officer

DISTRIBUTION:  
DIR  
D/DIR  
EXEC DIR  
DDP  
DDO

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

Encl:  
a/s

~~Classified By NSA/GSCM 1292  
Declassify On: Originating Agency's Determination Required~~

~~TOP SECRET NOFORN~~

OPTIONAL FORM NO. 10  
(REV. 1-80)  
NSA FOIA Case 100386 Page 00437  
U.S. GPO: 1985-201-750/50101

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET-HANDLE VIA COMINT CHANNELS ONLY-NOFORN~~

A PERSPECTIVE ON THE UKUSA SIGINT RELATIONSHIP

~~THIS DOCUMENT IS TOP SECRET-HANDLE VIA COMINT CHANNELS ONLY-NOT  
RELEASABLE TO FOREIGN NATIONALS IN ITS ENTIRETY.~~

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

I. SUMMARY

A. The roots of the UKUSA SIGINT agreement go back more than 50 years. Throughout these five decades it has been without question the most valuable partnership for both NSA and GCHQ. The past few years have been a watershed, however, marked by the collapse of the Soviet Union and Warsaw Pact on the one hand and [redacted] on the other. The reality of the one and eventuality of the other have had and will continue to have a significant impact on NSA operations and on our approach to dealing with GCHQ. [redacted]

[redacted]

C. This paper is a brief assessment of the current state of the UKUSA relationship from SUSL0L's perspective. [redacted]

[redacted]

~~TOP SECRET-HANDLE VIA COMINT CHANNELS ONLY-NOFORN~~

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

~~TOP SECRET-HANDLE VIA COMINT CHANNELS ONLY-NOFORN~~

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

II. UKUSA TODAY

A. The unexpected and rapid collapse of European communism has had a profound affect on NSA. The "peace dividand" has led to budget cuts, base closures, and manpower reductions. Despite this, we still have many more people and resources than GCHQ has or ever will have. GCHQ, on the other hand, continues to have key real estate, some very talented technical people, and (at least at present) a greater degree of financial flexibility.

B. BASE CLOSURES. As we have ceased operations in a number of European countries with the closing of [redacted]

[redacted]

C. MANPOWER. The need to significantly trim the NSA work-force over the next five years will have a profound affect on our ability to meet our customers' intelligence needs. [redacted]

[redacted]

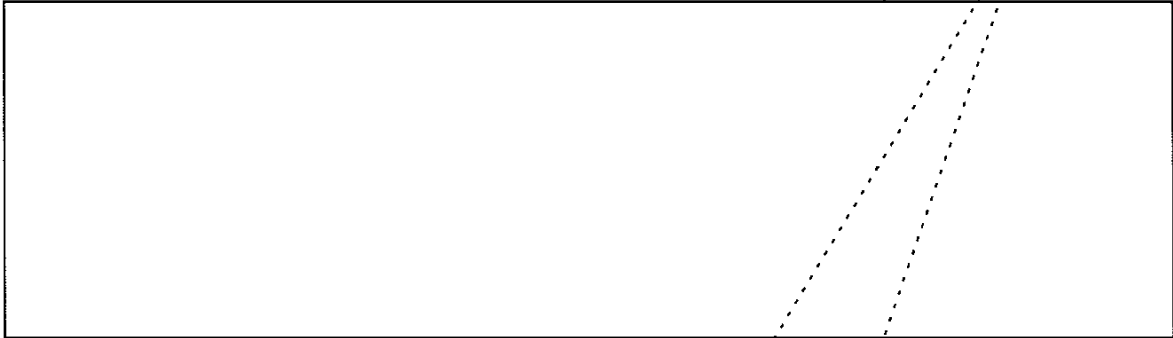
D. MONEY. Despite what continues to be a much larger budget, NSA's mandated cutbacks in spending have left us with much less financial flexibility than our British counterparts.

[redacted]

~~TOP SECRET-HANDLE VIA COMINT CHANNELS ONLY-NOFORN~~

(b) (1)  
(b) (3)-18 USC 793  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36

~~TOP SECRET-HANDLE VIA COMINT CHANNELS ONLY-NOFORN~~

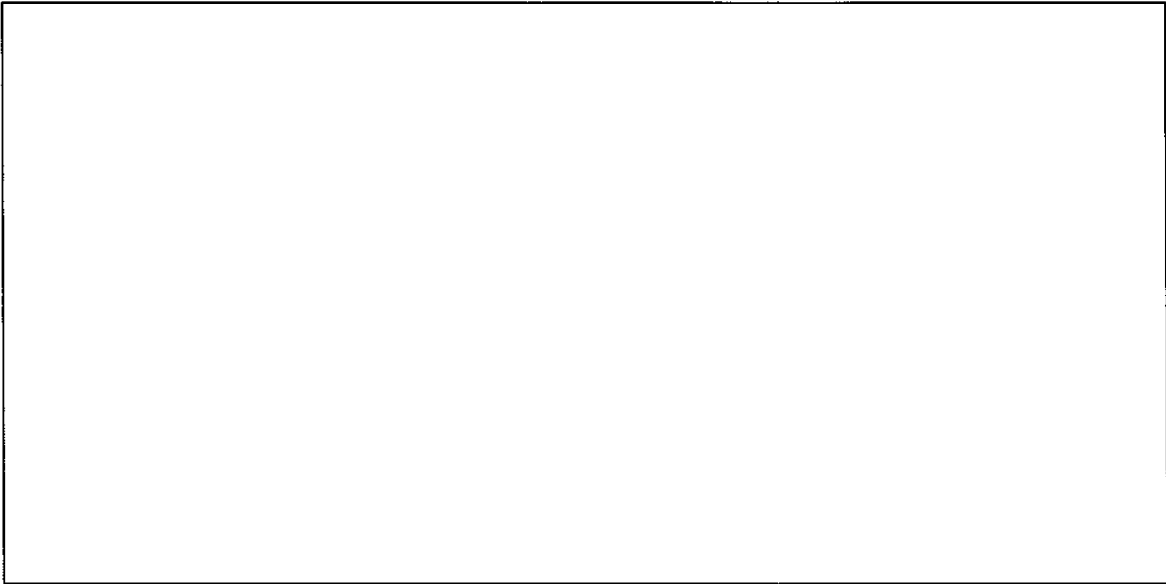


III. THE CHALLENGE OF CHANGE

A. Where each side has gained a great deal as a result of our long partnership, we believe it is becoming more important to NSA than ever before. The geography offered by GCHQ within the



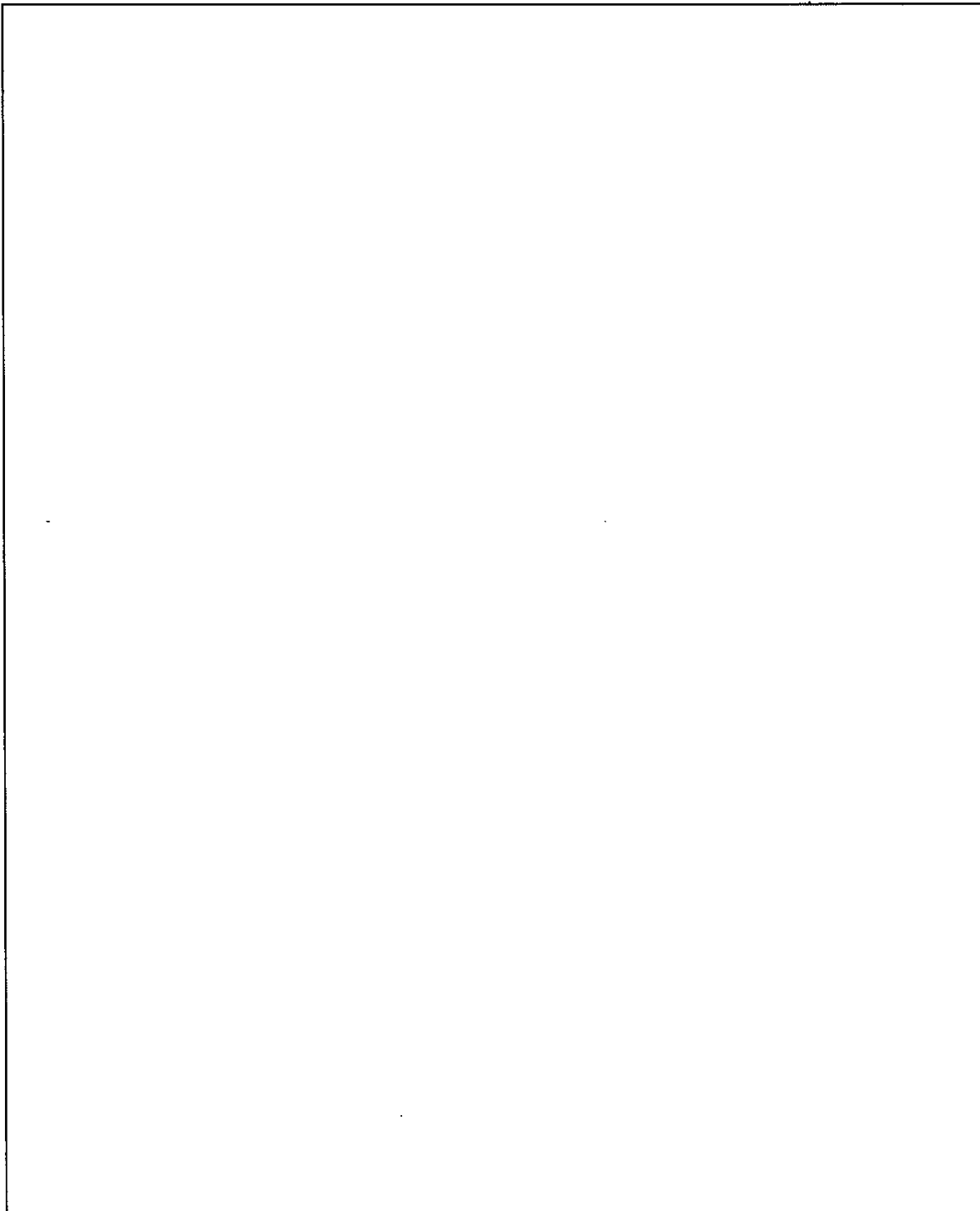
B. There are three major strands that hold the potential of altering the nature of our special relationship:



~~TOP SECRET-HANDLE VIA COMINT CHANNELS ONLY-NOFORN~~

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

~~TOP SECRET HANDLE VIA COMINT CHANNELS ONLY NOFORN~~



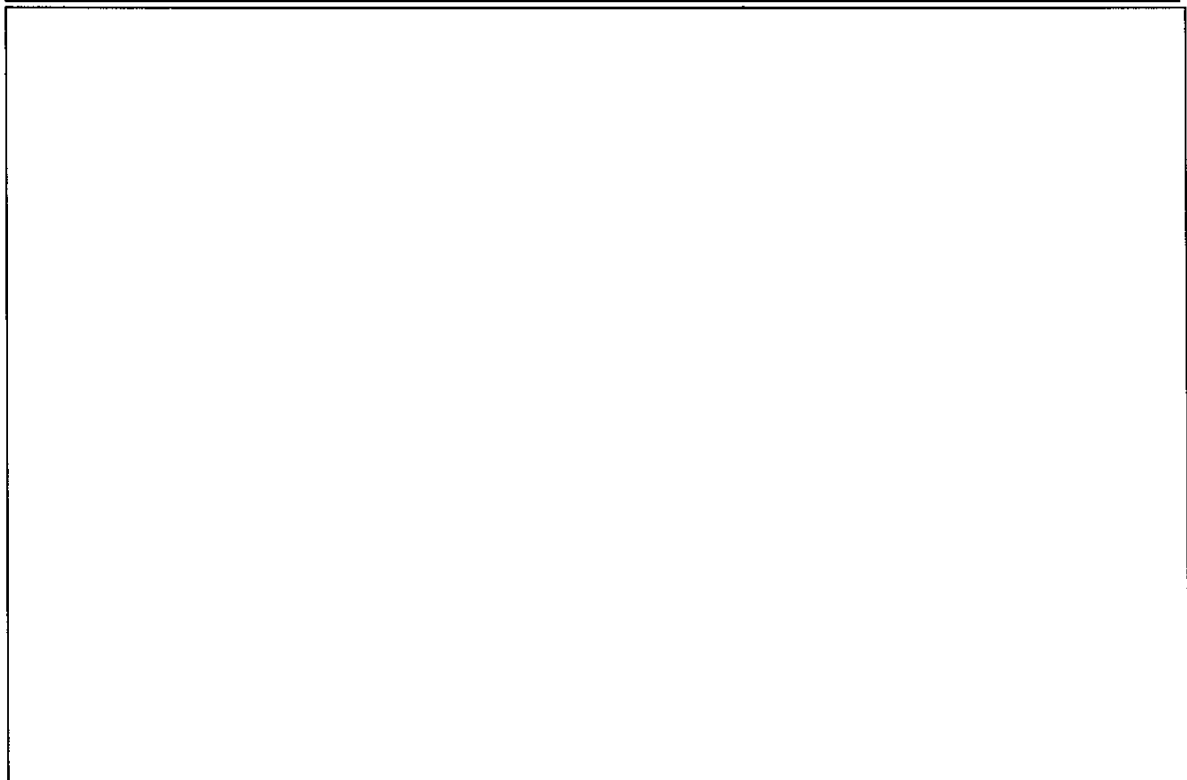
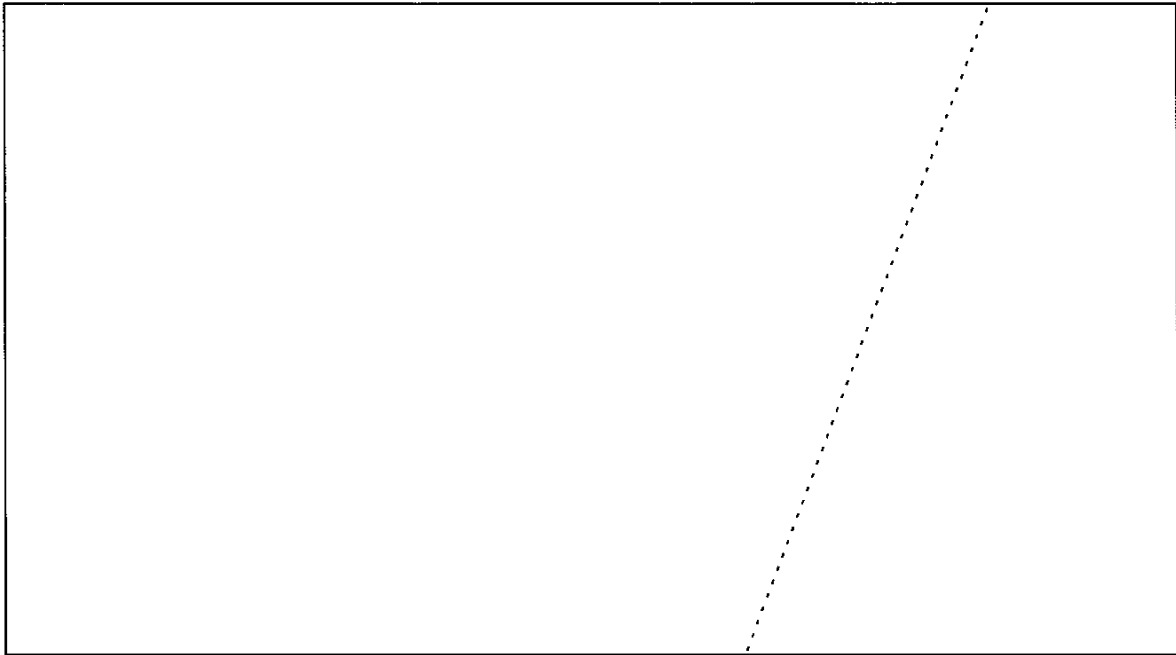
~~TOP SECRET HANDLE VIA COMINT CHANNELS ONLY NOFORN~~

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

F.8 '11

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

~~TOP SECRET HANDLE VIA COMINT CHANNELS ONLY NOFORN~~



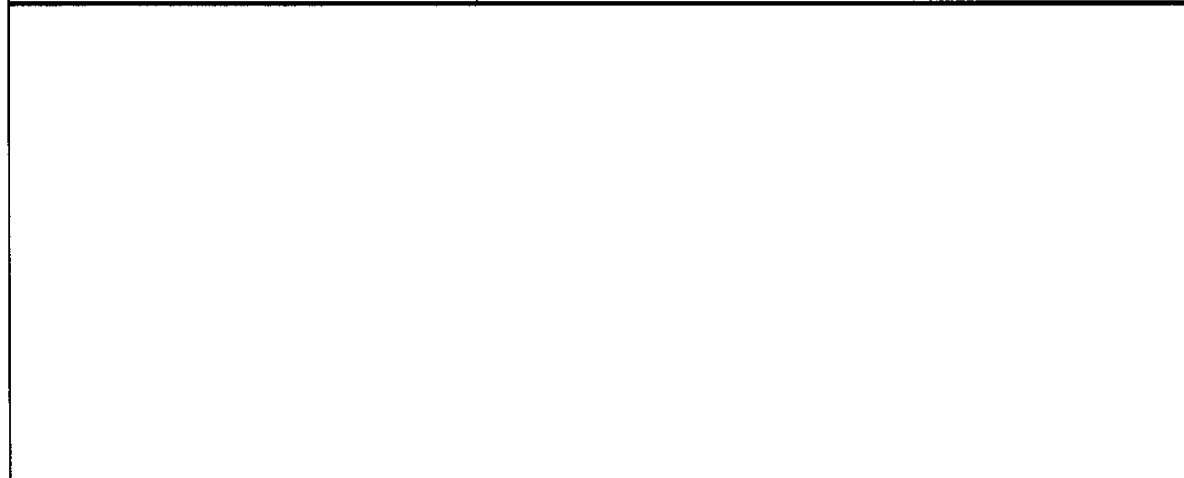
~~TOP SECRET HANDLE VIA COMINT CHANNELS ONLY NOFORN~~

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

~~TOP SECRET HANDLE VIA COMINT CHANNELS ONLY NOFORN~~



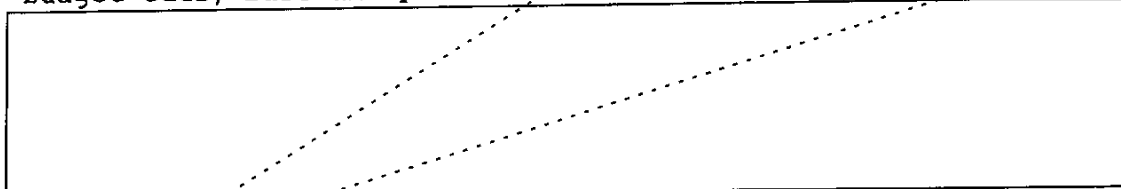
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36



IV. MANAGING THE FUTURE

A.

The changes outlined in the above pages; the end of the Cold war, budget cuts, base and personnel drawdowns and the



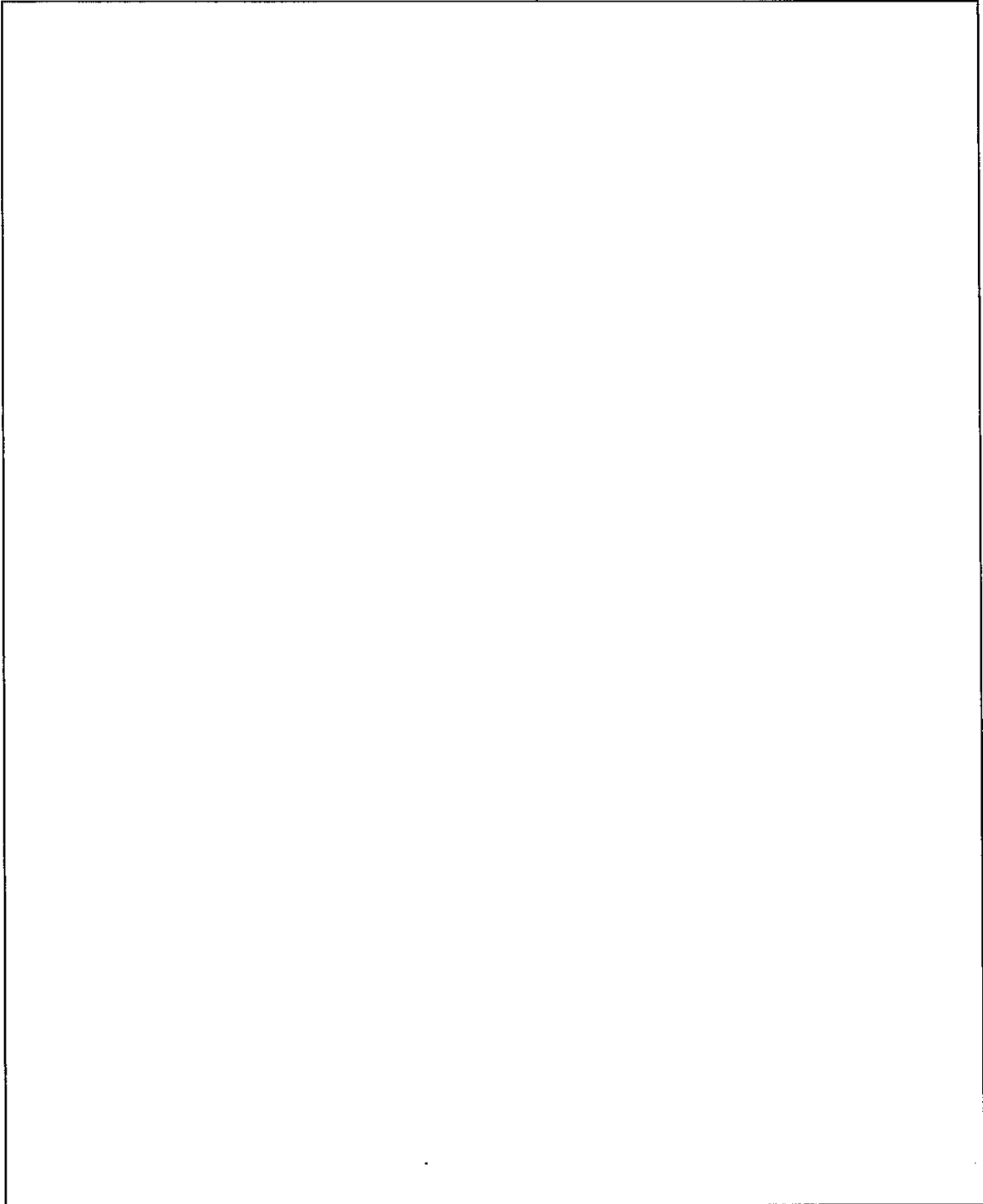
(b) (1)  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36

~~TOP SECRET HANDLE VIA COMINT CHANNELS ONLY NOFORN~~



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

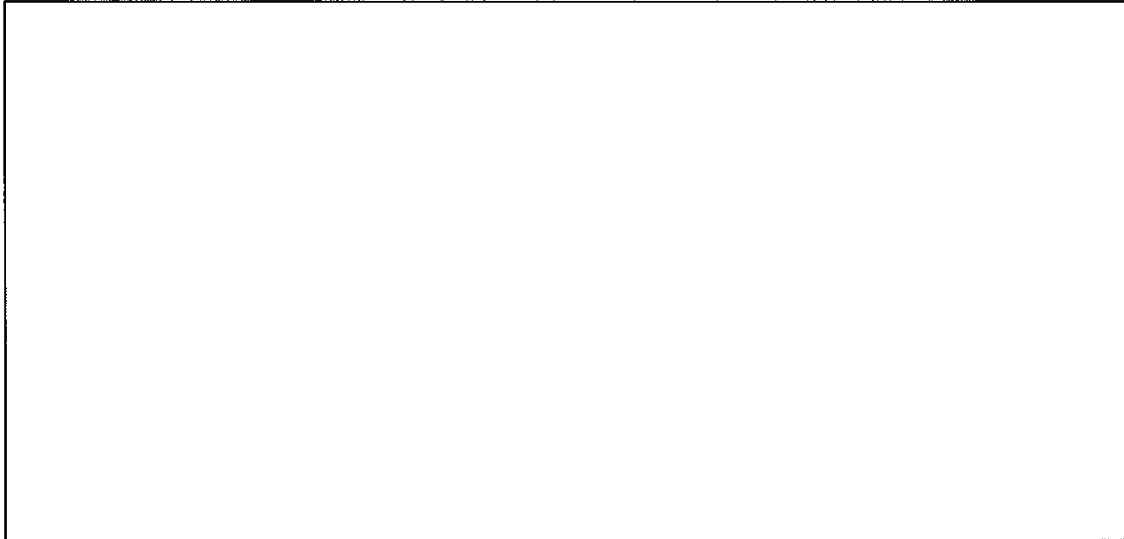
~~TOP SECRET-HANDLE VIA COMINT CHANNELS ONLY-NOFORN~~



~~TOP SECRET-HANDLE VIA COMINT CHANNELS ONLY-NOFORN~~

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

~~TOP SECRET-HANDLE VIA COMINT CHANNELS ONLY-NOFORN~~



6. The UKUSA relationship is so broad and so important that it may be inappropriate to treat it in the same way as other foreign relationships. It requires a higher level of visibility and more intense and organized management attention to all facets of the relationship.

7. Other areas of consideration may emerge as we begin to examine and manage the relationship more closely.

V. CONCLUSION

The UKUSA SIGINT relationship is the most important and productive one that we have. There is the potential for this relationship to change in the future



It is a challenge that should not be ignored.

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

~~TOP SECRET-HANDLE VIA COMINT CHANNELS ONLY-NOFORN~~

~~TOP SECRET~~  
UNITED KINGDOM  
Government Communications Headquarters (GCHQ)

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

BACKGROUND:

Nature of Relationship:

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

SIGINT:

[Redacted]

INFOSEC:

- INFOSEC exchange is more limited than SIGINT exchange, although

[Redacted]

U.S. Resources Required:

- No direct monetary transfer to GCHQ.

[Redacted]

NSA Objectives:

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

- The close relationship between NSA and GCHQ has always been useful when burden sharing divisions of effort are required to maximize intelligence collection.

[Redacted]

~~NOFORN~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

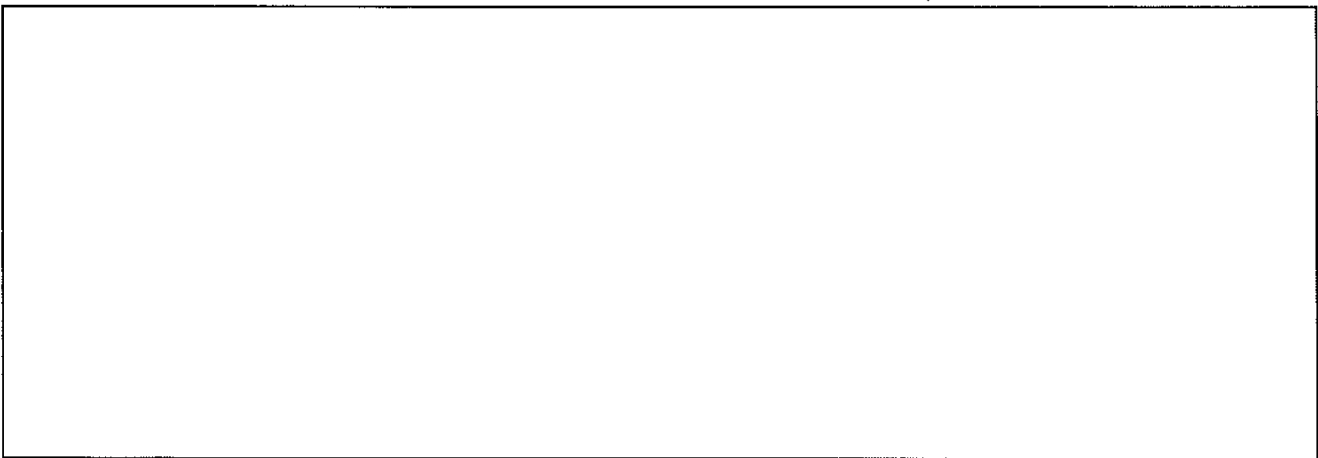
~~TOP SECRET~~

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

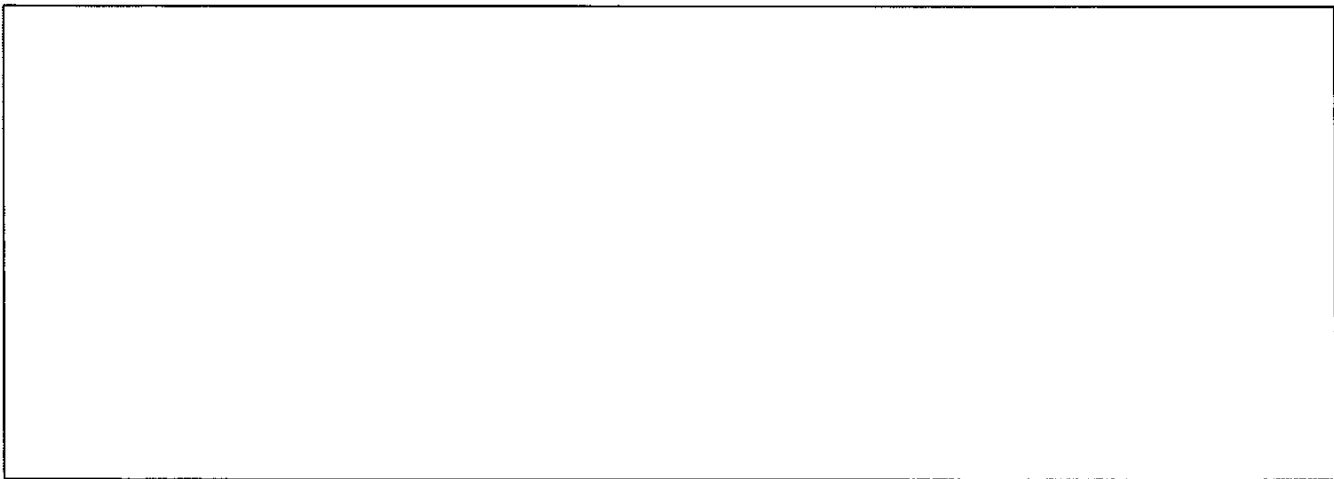
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

~~TOP SECRET~~

Assessment of Net Benefit to U.S.:



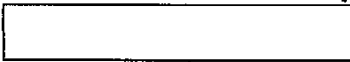
UNRESOLVED ISSUES:



RECOMMENDATIONS/DISCUSSION TOPICS/FUTURE PROSPECTS:

- Recommend agreement with forthcoming GCHQ proposal to hold UKUSA Third Party review in Spring 1994.
- Formulate comprehensive foreign policy for GCHQ to include [redacted] to ensure DIRNSA has full management perspective of ongoing and future collection objectives.

ORIGINATOR:



N521; -963-3745s, 2B1124, 20Oct93

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

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

~~NOFORN~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

~~TOP SECRET UMBRA~~

~~VRK-11/VRK-7/VRK-1~~  
~~VRK-109/VRK-310~~

SECURITY CLASSIFICATION

SPECIAL DOCUMENT ROUTING SLIP  
(Requires Special Handling)

FROM  DDO	TO  DDPP	DATE  14 March 1984
-----------------	----------------	---------------------------

SUBJECT  
  
"What We Want Our Second Parties To Do For Us"

NAME	DISPOSITION	INITIAL	DATE

CONTROL NUMBER

FORM A4578 REV APR 78 (Supersedes A4578 NOV 58 which is obsolete) SECURITY CLASSIFICATION

~~NOFORN~~

~~TOP SECRET UMBRA~~

Approved for Release by NSA on  
09-20-2018, FOIA Litigation Case #100386

DATE: 22 March 1984

REPLY TO  
ATTN OF: DDO

SUBJECT: CMR VI Tasks (U)

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

TO: DDPP

~~THIS MEMORANDUM AND THE ENCLOSURES ARE CLASSIFIED TOP  
SECRET UMBRA NOFORN [redacted]  
IN ITS ENTIRETY~~

1. Reference your DDPP-446-83, same subject, 4 January 1984.  
The following is submitted in response to your query regarding "What  
do we want our Second Parties to do for us?".

2. The recommended initiatives are listed in six categories,  
ranging from major areas of desire/need [redacted] to areas where  
improvement is needed [redacted]

In addition, unique subject areas are contained such as: [redacted]  
[redacted] Move of [redacted] Relocating the

3. Themes that dominated the requests: [redacted]

(b) (1)  
(b) (3)-18 USC 793  
(b) (3)-50 USC 3024 (1)  
(b) (3)-P.L. 86-36

*[Signature]*  
C. R. LORD  
Deputy Director  
for  
Operations

Encl:  
a/s

~~Classified By NSA/CSSM 123-2~~  
~~Declassify On: Originating Agency's Determination Required~~

OPTIONAL FORM NO. 10  
(REV. 1-80)  
GSA FPMR (41 CFR) 101-11.6  
5010-114

NOFORN

~~TOP SECRET UMBRA~~

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

[Redacted]

GCHQ

DSD/GCSB

CSE

[Large Redacted Area]

~~NOFORN~~

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

[Redacted]

GCHQ

DSD/GCSB

CSE

[Large Redacted Area]

~~NOFORN~~



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

[Redacted]

GCHQ

DSD/GCSB

CSE

[Large Redacted Area]

~~NOFORN~~

Doc ID: 6636836  
(b) (3) - 18 USC 798  
(b) (3) - 50 USC 3024 (i)  
(b) (3) - P.L. 86-36

~~VRK-11/VRK-7/VRK-1/VRK-10/VRK-310~~

[Redacted]

GCHQ

DSD/GCSB

CSE

[Large Redacted Area]

~~NOFORN~~

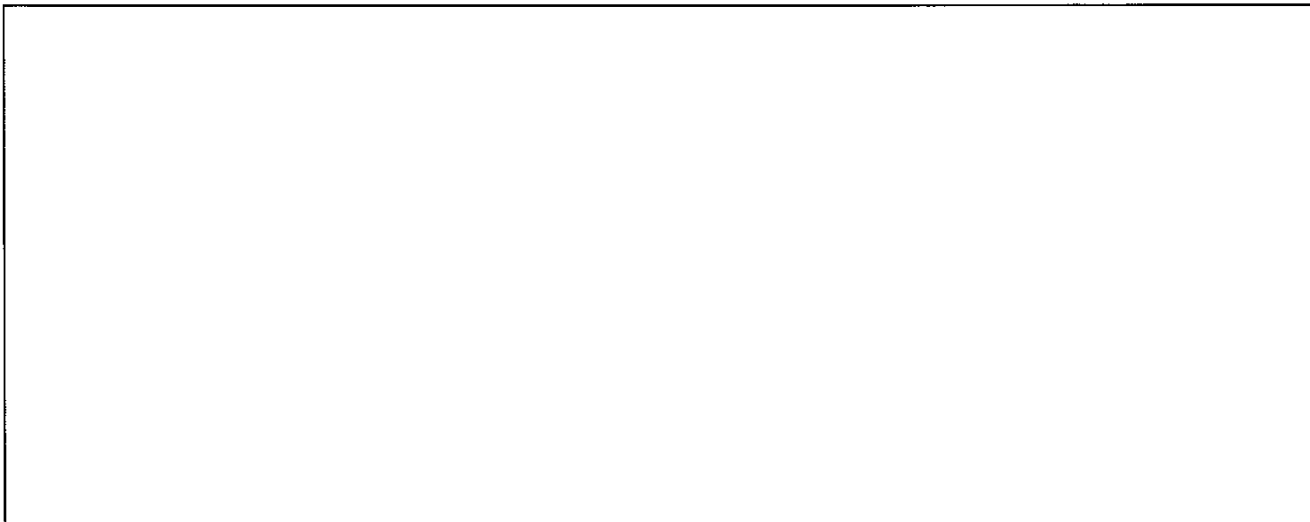
~~TOP SECRET UMBRA~~



GCHQ

DSD/GCSB

CSE



(b) (1)  
(b) (3) - 18 USC 798  
(b) (3) - 50 USC 3024 (i)  
(b) (3) - P.L. 96-36

~~NOFORN~~

~~TOP SECRET UMBRA~~

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

[Redacted]

GCHQ

DSD/GCSB

CSE

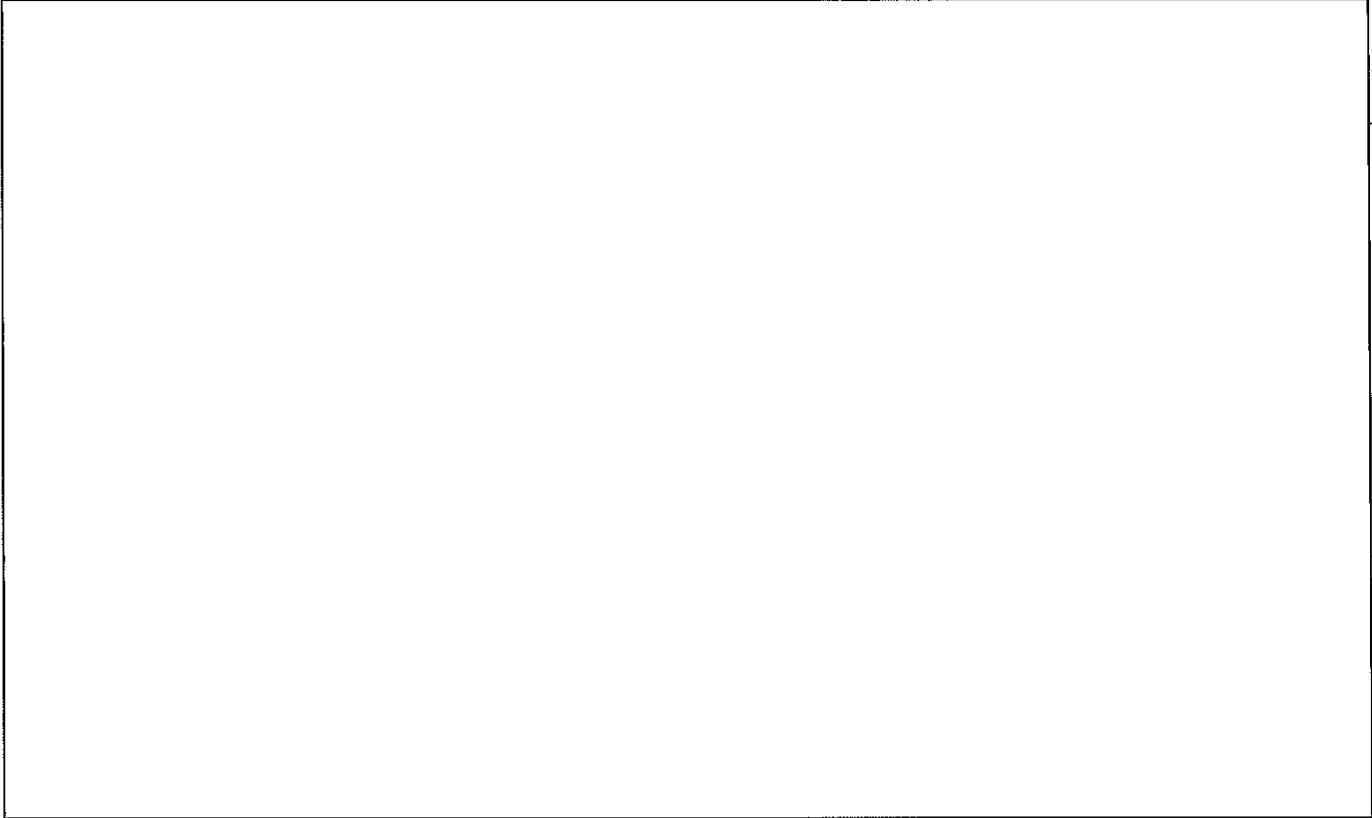


~~NOFORN~~

GCHQ

DSD/GCSB

CSE



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

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

[Redacted]

GCHQ

DSD/GCSB

CSE

[Large Redacted Area]

~~NOFORN~~

~~TOP SECRET UMBRA~~

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

[Redacted]

GCHQ

DSD/GCSB

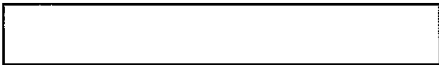
CSE



~~NOFORN~~



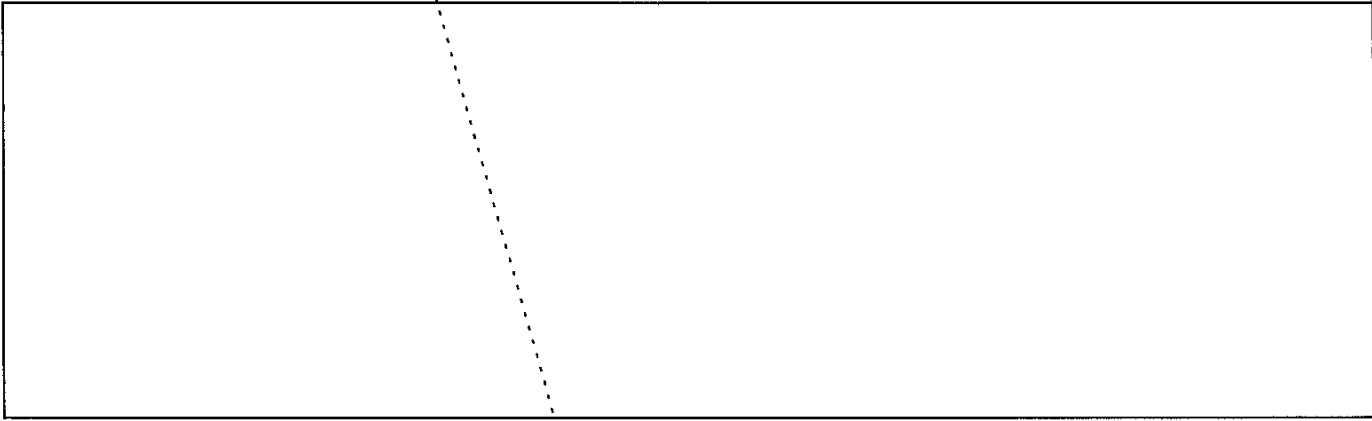
(b) (1)  
(b) (3)-18 USC 798  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36



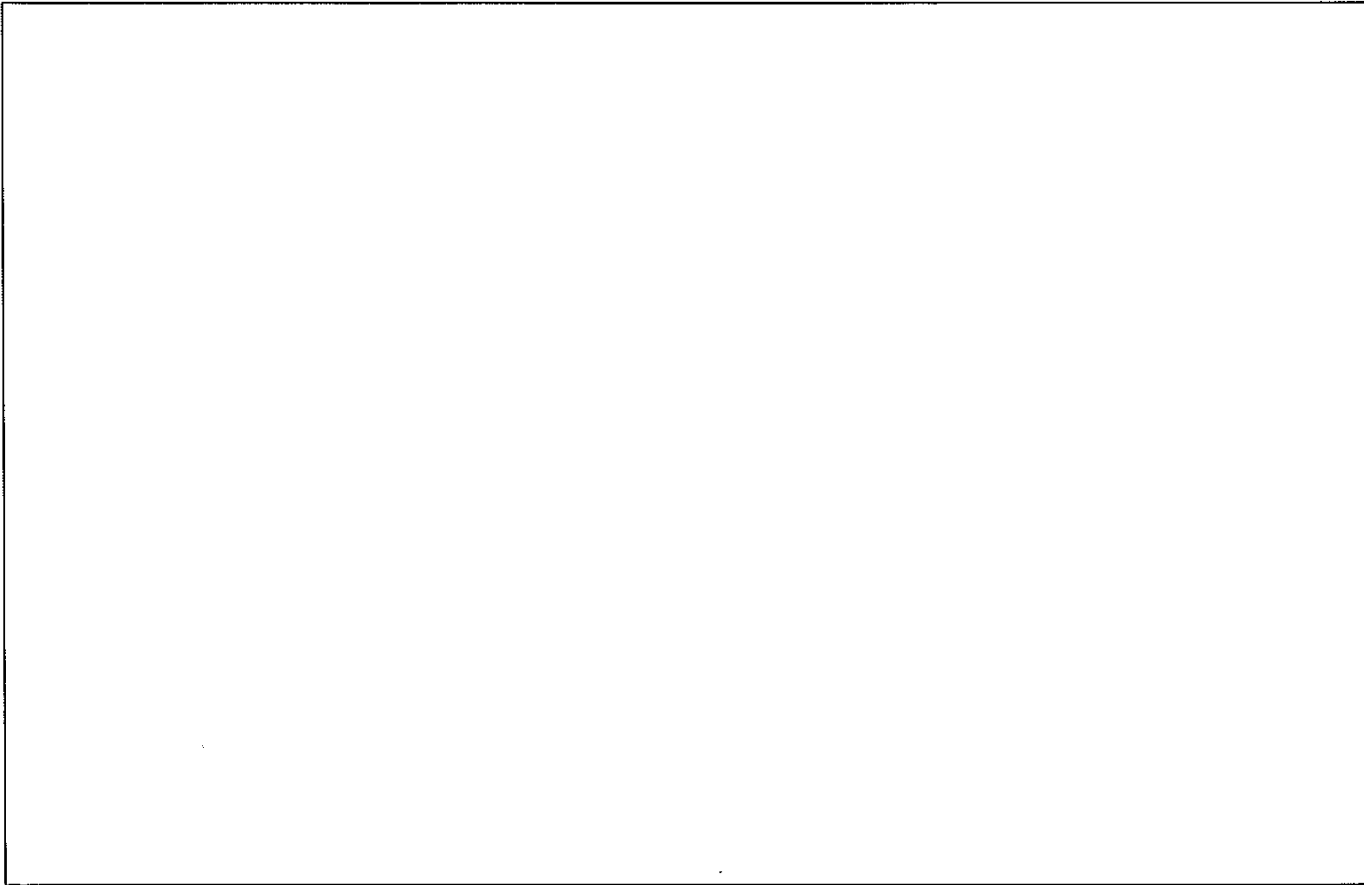
GCHQ

DSD/GCSB

CSE



Operations Center at GCHQ



~~NOFORN~~

~~TOP SECRET~~

# memorandum

DATE: 21 DEC 1984

REPLY TO  
ATTN OF: DDO

SUBJECT: Kerr Committee Study of SIGINT Relationships with the  
~~United Kingdom~~ INFORMATION MEMORANDUM (U)

TO: DDPP

Reference Q32-245-84, subject as above, 17 September 1984.  
The attached document contains information for your use in  
responding to the Kerr Committee on U.S.-U.K. SIGINT Arrangements.



C. R. LORD  
Deputy Director  
for  
Operations

Encl:  
a/s

~~ALL INFORMATION CONTAINED  
HEREIN IS UNCLASSIFIED EXCEPT  
WHERE SHOWN OTHERWISE~~

~~HANDLE VIA  
TALENT-KEYHOLE-COMINT  
CONTROL SYSTEMS JOINTLY~~

~~CLASSIFIED BY MULTIPLE SOURCES~~

~~NOFORN~~

OPTIONAL FORM NO. 10  
(REV. 1-80)  
GSA FPMR (41 CFR) 101-11.6  
5010-114

GPO : 1984 O - 439-419

~~TOP SECRET~~

NSA FOIA Case 100386 Page 00461

~~TOP SECRET UMBRA~~

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

U.S.-UNITED KINGDOM SIGINT ARRANGEMENTS (U)

1. ~~(S-EO)~~ The SIGINT collaboration with the United Kingdom began in 1941 and was formalized in the UKUSA agreement of 1946. The many parallel material interests and intelligence objectives that dictated mutual cooperation have developed and grown to an almost completely integrated sharing partnership. This SIGINT relationship is part of a partnership which also includes Australia, New Zealand, and/or Canada's involvement in certain initiatives. The principles embodied in this agreement have not changed and the working relationship between NSA and the U.K. Government Communications Headquarters (GCHQ) has continued to be mutually beneficial to both partners in satisfying their respective national requirements. The arrangement now encompasses combined working parties, exchange of liaison officers, and assignment of analysts to integrated posts and entails close collaborative approaches to collection, analysis, and reporting. In addition, Divisions of Effort (DOE) and/or understandings between NSA and GCHQ are undertaken to respond to existing requirements.

2. ~~(TSC TK NF)~~ In general, DOE's and/or understandings between NSA and GCHQ encompass the sharing of collection, processing, and reporting on targets worldwide, ranging

[Redacted]

Examples of specific arrangements on these targets are:

[Redacted]

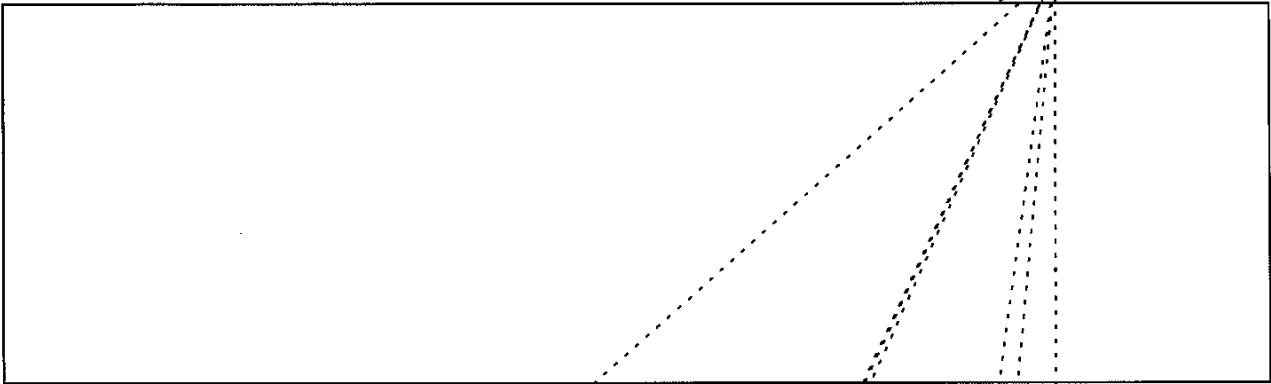
~~HANDLE VIA~~  
~~TALENT KEYHOLE COMINT~~  
~~CONTROL SYSTEMS JOINTLY~~

~~CLASSIFIED BY MULTIPLE SOURCES~~

~~TOP SECRET UMBRA~~ Case 100385 Doc 00462

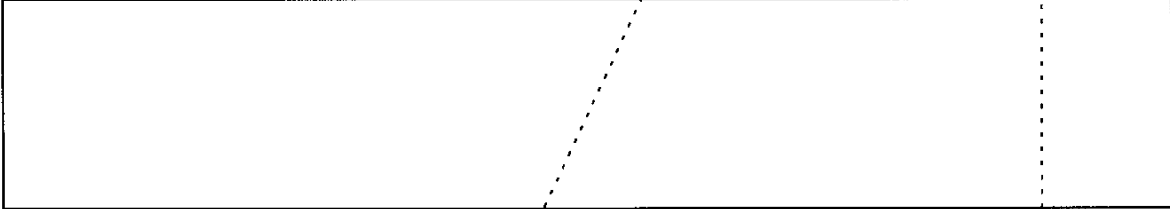
~~TOP SECRET UMBRA~~

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



3. ~~(TSC)~~ The U.S. receives information from the U.K. similar to that which we provide. This includes product and technical reports/feedback, raw traffic, data base access on worldwide internal and external communications for the majority of the countries worked at NSA, (including [redacted] and terrorist activity communications). Collection of these communications by both nations is acquired by [redacted]

[redacted] COMINT, ELINT and TELINT. In the exploitation of certain targets, complete collaboration exists between the two headquarters in satisfying collection and reporting efforts. Since this approach has a positive affect on required resources and involves full sharing of acquired information, these exchange arrangements are beneficial to both NSA and GCHQ. Examples of this close cooperation include [redacted]



4. ~~(S-CCO)~~ Formal message exchanges and informal coordination procedures exist for collection, processing, and reporting. There is a constant exchange of technical information and a common data base is shared, where possible, to avoid duplication of effort. The program involving analyst-to-analyst visits between the two headquarters has been most beneficial, as well as GCHQ's participation in meetings elsewhere [redacted]

[redacted] High-level planning conferences are also held to officially address proposed changes to the relationship. In addition to the defined areas of responsibility, U.S. members are integrated into the GCHQ organization, and vice versa, to ensure articulation of concerned priorities and requirements.

~~HANDLE VIA~~  
~~TALENT KEYHOLE COMINT~~  
~~CONTROL SYSTEMS JOINTLY~~

~~NOFORN~~

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

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

5. ~~(S-NOFORN)~~ A free exchange of information exists on targets of mutual interest. [redacted]

[redacted]

6. ~~(S-CCO)~~ Other benefits we receive from our relationship with the U.K. are:

- freedom to apply valuable resources to other areas of interest which would be impossible or considerably more expensive without mutual agreements;

- Manpower to assist advanced program collection, operations, and support (e.g., transcriber - analysts to work specified problems);

[redacted] at GCHQ to help with responses to national and time-sensitive requirements regarding [redacted]

[redacted]

[redacted]

7. ~~(S-CCO-NF)~~ There are no major problems that we are aware of in the security procedures employed by GCHQ to protect SIGINT and U.S. and/or U.K.'s methods and sources. [redacted]

[redacted]

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

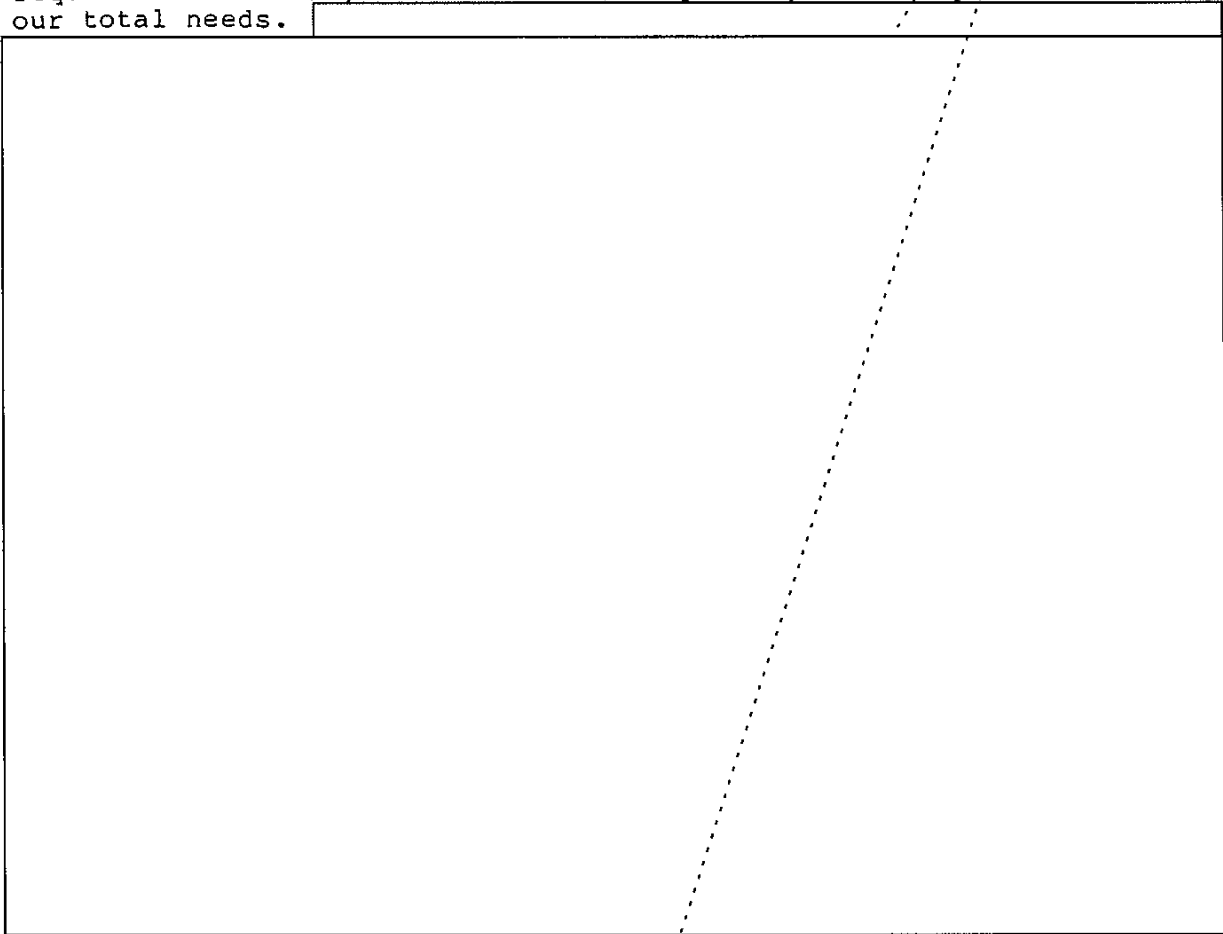
~~HANDLE VIA~~  
~~TALENT KEYHOLE COMINT~~  
~~CONTROL SYSTEMS JOINTLY~~

~~TOP SECRET UMBRA~~

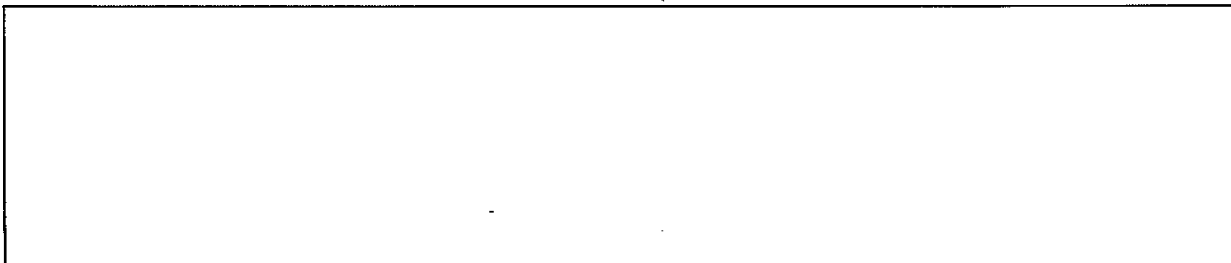
~~TOP SECRET UMBRA~~

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

8. ~~(TSC-TK-NF)~~ In general, the value of this relationship is extremely high and allows for a much fuller analytic effort than that possible with only U.S. resources. As previously mentioned, the exchanges of information combined with unique British collection and analysis efforts contribute greatly to the NSA mission. GCHQ consistently provides valuable input to the satisfaction of U.S. requirements and is, in most cases, cooperative and responsive to our total needs.



9. ~~(S-CCO)~~ Following are current trends for the future to expand this relationship:

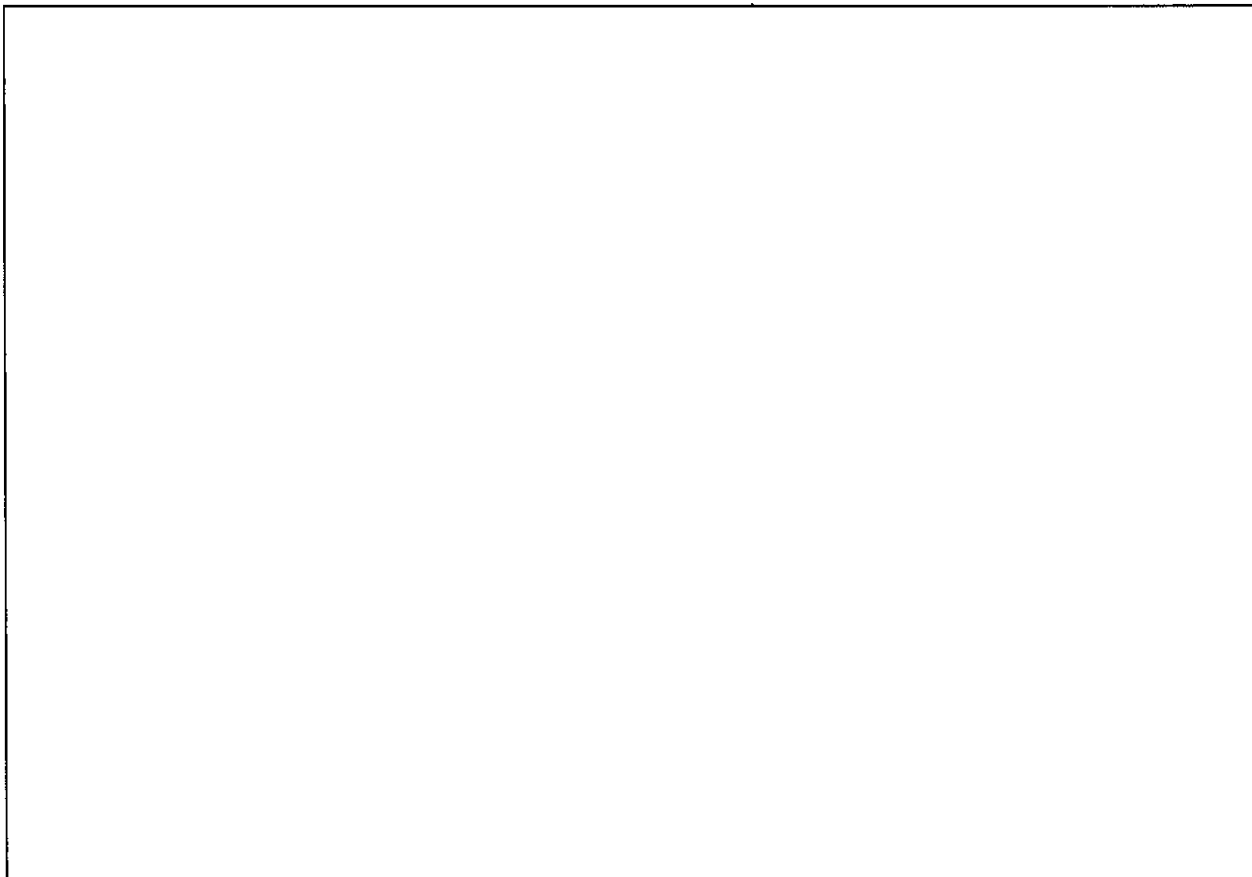


~~HANDLE VIA~~  
~~TALENT-KEYHOLE-COMINT~~  
~~CONTROL SYSTEMS JOINTLY~~

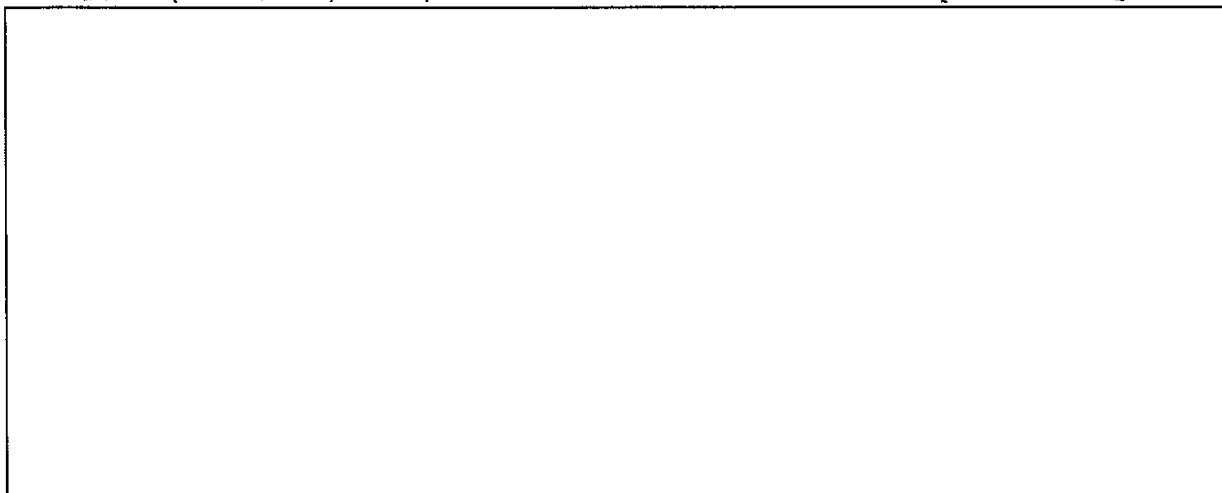
~~TOP SECRET UMBRA~~

~~NOTORN~~

~~TOP SECRET FRODOBA~~



10. ~~(S CCO NF)~~ Current issues in our relationship with GCHQ



(b) (1)  
(b) (3)-18 USC 793  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

~~HANDLE VIA~~  
~~TALENT KEY HOLE COMINT~~  
~~CONTROL SYSTEMS JOINTLY~~

~~TOP SECRET FRODOBA~~ NSA FOIA Case 100386 Page 00466

~~TOP SECRET // COMINT // NOFORN // X1, X5, X6 //~~

Date: 18 Feb 00

## FOREIGN PARTNER STRATEGIC PLAN

### UNITED KINGDOM

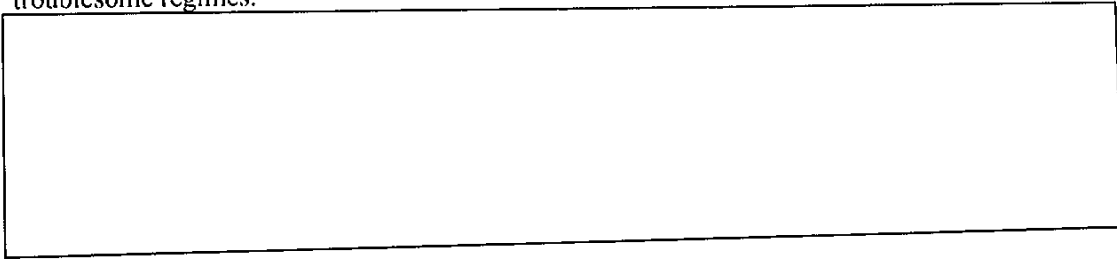
#### I. U.S. POLICY OBJECTIVES

\* Our closest ally - continue close cooperation to achieve U.S. foreign policy objectives on shared concerns world-wide.



#### II. U.S. INTELLIGENCE OBJECTIVES (NON-SIGINT EQUITIES)

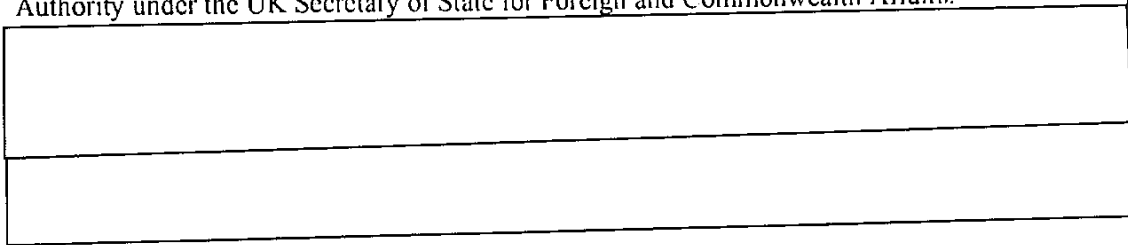
\* Continue strong analytical sharing concerning key global and regional issues and troublesome regimes.



#### III. UK GOVERNMENTAL INSTITUTIONS AND POLICY

##### A. SIGINT

\* Government Communications Headquarters (GCHQ) is the UK's National SIGINT Authority under the UK Secretary of State for Foreign and Commonwealth Affairs.



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

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

~~TOP SECRET // COMINT // NOFORN // X1, X5, X6 //~~

NSA FOIA Case 100386 Page 00467



~~TOP SECRET // COMINT // NOFORN // X1, X5, X6 //~~

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

B. INFOSEC

- \* The UK is the U.S.'s key partner for INFOSEC.
- \* The Communications Electronics Security Group (CESG), equivalent to NSA's Information Systems Security Organization (ISSO) is integrated within GCHQ and is responsible for keeping its governments communications and computer systems secure.
- \* Each is its respective government's national technical authority for Information Security (INFOSEC).

\* CESG and the ISSO have a long-standing relationship. [redacted]

[redacted]  
\* A growing need for information systems interoperability has expanded this relationship to include open exchanges on emerging technologies and planned joint evaluations of INFOSEC products.

\* Future information systems interoperability problems, whether they be in bilateral, NATO or coalition environments, cannot be solved without partnering with our closest ally.

\* Virtually no future real-world scenario, peace-making or peace-keeping, can be imagined without both U.S. and UK involvement.

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

C. UK's NATIONAL SECURITY POLICY

\* As a member of NATO, the UK is the closest U.S. ally and partner on European security issues and in peacekeeping coalition activities on the continent.

[redacted]

IV. CURRENT CRYPTOLOGIC RELATIONSHIP

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

A. REPRESENTATION:

\* NSA is represented to the UK through its SUSLOL personnel. [redacted]

[redacted]

~~TOP SECRET // COMINT // NOFORN // X1, X5, X6 //~~

~~TOP SECRET // COMINT // NOFORN // X1, X5, X6 //~~

B. MILITARY TO MILITARY

\* See below under U.S. objectives.

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

C. U.S. OBJECTIVES:

\* Maximize sharing of intelligence product between NSA and GCHQ to guarantee vital information for U.S. and UK customers.

\* Focus the combined UKUSA efforts to best effect against the highest priority targets/ subjects.

\* Nurture cooperation in cryptographic products, and special programs.

\* [Redacted]

\* Ensure that GCHQ technology, architectures, and connectivity remain fully compatible with those of the U.S. Cryptologic System.

\* Develop practical divisions of effort between NSA and GCHQ to maximize our mutual intelligence productivity and make optimal use of scarce resources.

\* Facilitate discussions among GCHQ, NSA, and the U.S. and UK military forces to expand SIGINT support to coalition forces.

\* Coordinate with CESG on secure communications solutions in emerging areas of interest such as [Redacted]

\* Continue to strengthen the CESG/ISSO INFOSEC relationship so that interoperability remains a top priority for critical infrastructure areas like key management and distribution and algorithm design and development.

\* Partner to produce interoperable INFOSEC products for the NATO and coalition environments, as well as bilaterally-interoperable products.

D. UK OBJECTIVES:

\* Sustain a renewed sense of strategic direction for GCHQ.

\* Maintain the focus on the customer.

\* Pursue the SINEWS (Sigint's New System) program in a way that transforms systems, working methods, and skills in order to exploit new intelligence opportunities/capabilities and meet the challenges of the global IT revolution.

\* Develop in both scale and impact GCHQ's contribution in the field of Information Operations at each of the policy, technical and operational levels.

\* CESG - expand the customer base for INFOSEC services.

\* Leverage resources, especially manpower, within CESG and ISSO, so that through a judicious division of labor and the use of intregrees, the research and development of future INFOSEC solutions can continue to the benefit of both countries.

~~TOP SECRET // COMINT // NOFORN // X1, X5, X6 //~~

~~TOP SECRET // COMINT // NOFORN // X1, X5, X6 //~~

V. RESOURCE AND BUDGETARY CONSIDERATIONS

[Redacted]

VI. CONTRIBUTIONS AND VALUE

[Redacted]

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

\* Exchanges on processing techniques.

[Redacted]

\* Strong diagnostic skills.

[Redacted]

\* Joint evaluation of INFOSEC products.

\* Collaborative work in INFOSEC research and development.

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

VII. CURRENT ISSUES

[Redacted]

VIII. PROSPECTS FOR THE FUTURE

\* Maintain, at a minimum, the current level of critical coverage and access afforded the U.S. via GCHQ collection.

\* Foster GCHQ capabilities with a focus on the newest technology targets.

\* Expand NSA-GCHQ secure connectivity at every level.

~~TOP SECRET // COMINT // NOFORN // X1, X5, X6 //~~

~~TOP SECRET // COMINT // NOFORN // X1, X5, X6 //~~

- \* Unify NSA/GCHQ cryptologic functions.
- \* Maintain cryptanalytic capability.
- \* Ensure effective UKUSA support to joint/combined operations.
- \* Sustain UKUSA technological superiority.
- \* Continue ISSO/CESG cooperation [redacted]
- \* Increase ISSO/CESG cooperation on INFOSEC interoperability issues for bilateral, NATO and coalition environments. [redacted]
- \* Improve collaboration in the diagnosis/attack development arena.

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

[redacted]

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

~~TOP SECRET // COMINT // NOFORN // X1, X5, X6 //~~

~~TOP SECRET VRK11 TK AG DC MC~~  
~~NOFORN~~

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

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

AN ASSESSMENT OF THE UKUSA RELATIONSHIP:  
WHERE WE GO FROM HERE

~~(S-NF)~~ The UKUSA relationship has been of inestimable value to NSA and cannot be abandoned, [redacted]

[redacted]

[redacted] This paper is an honest effort by SUSLO-4 to describe the strengths and weaknesses of the UKUSA relationship so that NSA might better be able to make some hard decisions about the future of the relationship.

~~(TS-NF)~~ There is no doubt that UKUSA offers NSA much. Just to document a few important contributions we must include:

[redacted] unique collection from GCHQ conventional sites, freeing US resources; use of UK [redacted] where the US has none; [redacted]

[redacted] the compatibility and interoperability of US & UK SIGINT systems; a strong analytic workforce, with a capability for independent interpretation of events; an especially competent cryptanalytic workforce; savings in US resources by analytic divisions of efforts; the pooling of resources on key technical projects during austere fiscal periods; [redacted]

[redacted] and, perhaps most important, a record of supporting the US as an ally in confronting world problems.

~~(S-NF)~~ Despite these outstanding areas of success, there

[redacted]

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

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

**Page Denied**

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

**Page Denied**

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

**Page Denied**



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

**Page Denied**

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

**Page Denied**

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

**Page Denied**

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

**Page Denied**

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

**Page Denied**

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

**Page Denied**

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

~~(S NF)~~

[Redacted]

~~(S NF)~~

[Redacted]

~~(S NF)~~

[Redacted]

INTERFACES

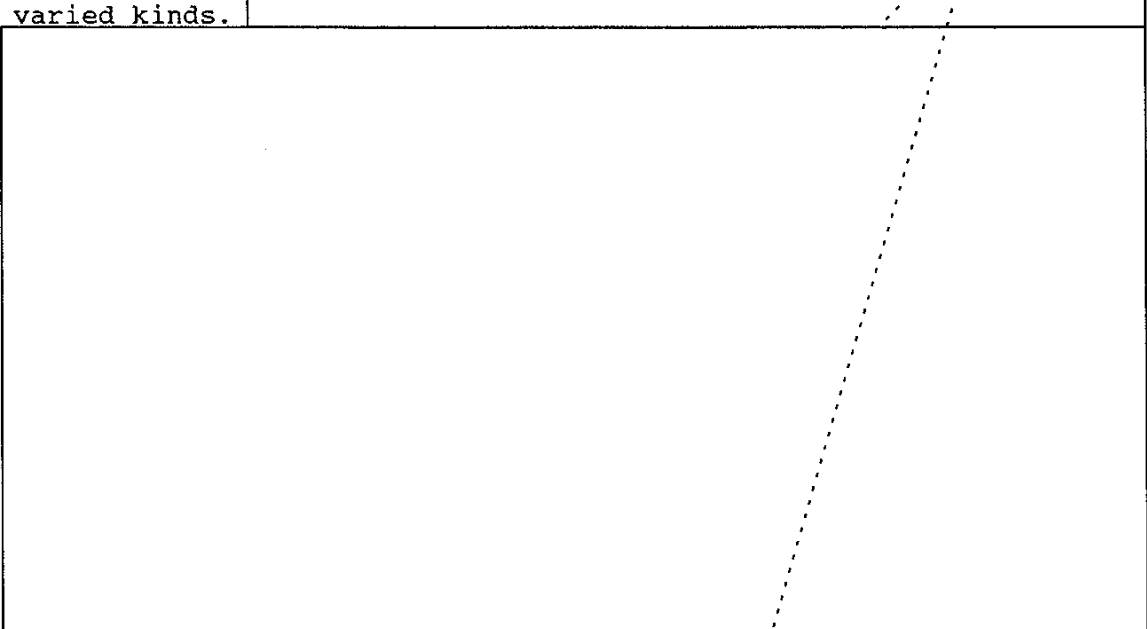
~~(C NF)~~ NSA and GCHQ interface in a number of ways, to include connection of joint processing systems, communications links of many types, and the exchange of personnel to work in integrated positions.

[Redacted]

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

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

~~(S-NF)~~ Communications between NSA and GCHQ run smoothly; both sides meet regularly to plan improved communications of varied kinds. [redacted]



~~(S-NF)~~ Aside from the respective liaison staffs, NSA and GCHQ exchange large number of integrees [redacted] NSA/CSS personnel at GCHQ; some [redacted] GCHQ integrees at NSA). Most integrees work hard at technical skills and contribute greatly to a mutual interchange of ideals and techniques that benefit both side greatly. More so in recent years, some operational and staff elements in GCHQ have begun to use integrees as their representatives, and some integrees have assumed liaison-like functions. Making matters worse has been a recent trend to send integrees to function as special assistants, sometimes to alpha plus-one components working sensitive missions. While they are no doubt of great help to NSA managers, they also serve as lobbyists for GCHQ seniors in policy matters. Recently GCHQ/K1 lobbied hard to place an integree in the G2/SA position. G2 rightly rejected this as it would give GCHQ insight into certain sensitive operations we do not share. In another instance a strategically placed GCHQ integree drafted an MOA that committed [redacted] assistance from NSA to GCHQ -- without addressing the correctness of this assistance, the propriety of this situation is disturbing.

~~(S-NF)~~ Whether comms links or exchange of integrees, the mode of interfacing with GCHQ evolves based on a myriad of decisions at various levels within NSA. Do we need to have an overall policy to ensure that these agreements are consistent with our plans for the future? For instance, should we determine a modus vivendi for exchange of integrees? Should the type of work be limited by charter? Should there be a common NSA position on the number and kind of electronic interfaces between NSA and GCHQ? Should the number be driven by NSA design or by GCHQ needs?

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



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

**Page Denied**

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

**Page Denied**

15 May 1984

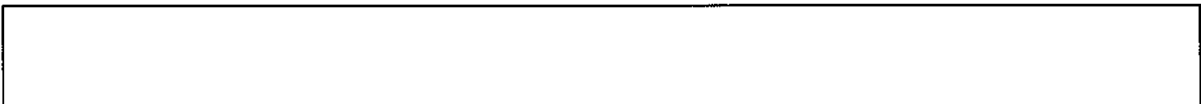
**CORPORATE-LEVEL PRINCIPLES ESTABLISHING THE  
BASIS FOR DEALING WITH SECOND PARTIES**

**OBJECTIVE:**

Provide a set of agreed upon macro-level principles, strategies and specific actions which will guide NSA Senior Management in the conduct of Second Party arrangements. The approach will be established by the Director, NSA/Chief, CSS and his Senior Managers.

**CORPORATE-LEVEL PRINCIPLES:**

- ° Base the conduct of Second Party relationships upon U.S. national interests, cryptologic and otherwise.
- ° Establish agreement that bi-lateral cryptologic activities will be planned for and conducted within the context of jointly developed goals and objectives and joint senior management decisions.
- ° Recognize that although U.S. and Second Party national policies will, in general, be congruent there will exist a set of situations when national interests and policies will diverge. We can anticipate that although these instances will often strain the bi-lateral partnerships, the effects will most generally be temporary. However, certain national interests will be divergent over longer terms and for related cryptologic activities, safeguards, procedures and facilities must be developed which preserve their NOFORN character and minimize embarrassment to continuing relationships.
- ° Establish an acceptance, within the framework of the Second Party agreements, that each party may be asked and expected to support the partnership outside their own individual national requirements for the good of the partnership, especially when a unique opportunity or capability to contribute exists within one of the Second Party centers.



- ° Recognize the very real limitations and constraints each is forced to operate within; however, it has been demonstrated that, when the high priority of certain endeavors are mutually agreed to and supported by the U.S., major additions can be accommodated, e.g.

- ° Emphasize the value added to the Second Parties of the U.S. sourced information, establishing the U.S. position that our

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

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

~~RELEASABLE TO FOREIGN NATIONALS~~

~~Classified By NSA 2004 1172  
Declassify On: Originating Agency's Determination Required~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

NSA FOIA Case 100386 Page 00486

~~TOP SECRET~~

- ° Establish an understanding with the Second Parties that performance within the construct of agreements reached is a critical criterion for future Second Party participation in shared arrangements.
- ° Develop a greater acceptance on the part of the Second Parties that the cryptologic business is dynamic and requires flexibility on the part of all parties if joint success is to be increased. At least on critical SIGINT targets for which we depend on collaborating agencies, Second Parties must operate on the same "metabolic rate" as NSA, including 24-hour operations.
- ° Identify duplicative, low priority or non-productive efforts which do not support the partnership and take joint action to curtail or eliminate such activities at the earliest possible time.
- ° Provide where possible standardization and interoperability emphasizing the value of such concepts for all areas of exchange and cooperation. One area requiring immediate attention is those activities involved in and supporting SIGINT Support to Military Operations.

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

SECOND PARTY STRATEGIES:

- ° Expand [redacted] by obtaining Second Party commitments to [redacted]

- ° Identify [redacted] requirements and opportunities which could be satisfied by Second Parties. (DDO)

- ° Identify Second Party initiatives which offer such significant unique potential that senior level U.S. officials should seek the necessary resource support from Second Party governments. (DDO, DDR, DDT, DDC, CSC)

- ° Identify and document those R&D areas where Second Parties should conduct studies and/or undertake development. (DDR)

- ° Explore Second Party maintenance and configuration control of major software systems at jointly managed facilities to support a strategy of reducing U.S. costs for overseas contractors. (DDT)

- ° Identify and document Second Party efforts which should be curtailed or eliminated. (DDO, DDC, DDR, DDT)

- ° Develop as soon as possible a firm division of effort on [redacted] [redacted] to ensure that each collaborating center is collecting unique information. (DDO)

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

~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

~~TOP SECRET~~

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

- Endeavor to ensure that [redacted] collection and processing is complementary to, and not duplicative of, the U.S. SIGINT System. (DDO, DDR, DDT)
- Reexamine critically the current bi-lateral divisions of effort with the U.K. on [redacted] to reduce the impact of their [redacted] on the USSS. (DDO)
- Encourage Second Parties to expand significantly their access to national communications satellite systems, and to develop communications capabilities which are interoperable with those of the USSS, to enhance the capacity, flexibility, connectivity and transparency of SIGINT communications. (DDT)
- Develop among NSA and Second Party organizations a specific program which will enhance the endurance and survival of SIGINT support through a range of crises up to and including limited nuclear hostilities. (DDT)

~~Classified By NSA/AFSSM 1032  
Rept with the Original Agency's Determination Required~~

~~NOT RELEASABLE TO FOREIGN NATIONALS~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

~~TOP SECRET~~

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

### NSA'S CRYPTOLOGIC RELATIONSHIPS WITH SECOND PARTIES (U)

#### Relationship with the UK's Government Communications Headquarters (GCHQ) (U)

~~(TS-CCO-UO)~~ The U.S.-UK SIGINT relationship is the oldest and most productive of NSA's foreign partnerships. It is based on a formal "UKUSA Agreement," signed in 1946, which provides for unrestricted exchange of SIGINT except for those areas specifically excluded at the request of either party.

[Redacted]

The UK's intelligence requirements and priorities are largely convergent with those of the U.S., and GCHQ's collection/processing/reporting typically complements that of NSA.

[Redacted]

GCHQ offers geography [Redacted] and resources for state-of-the-art collection, processing, and analytic efforts.

[Redacted]

duplication and maximize coverage through joint sites and cross-tasking, despite site closures. GCHQ is NSA's only peer in the field of cryptomathematics and virtually all major advances within the field of cryptography have occurred as a result of our mutual sharing. As NSA supports U.S. Government efforts towards achieving a secure global information infrastructure, GCHQ stands as our most influential foreign partner in advancing INFOSEC policies in the international arena.

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

#### Relationship with Canada's Communications Security Establishment (CSE) (U)

~~(TS-CCO-UO)~~ The U.S.-Canada SIGINT relationship also dates back to World War II; the "CANUSA Agreement," signed in 1949, is an offspring of UKUSA. The basic tenet of CANUSA is cooperation in all aspects of SIGINT, "except when considered prejudicial to the rational interests of one of the parties." Canada has

[Redacted] which complement U.S. collection. They also have an active and productive program similar to our FISA-approved collection. Furthermore, CSE has hired talented engineers, computer scientists, and mathematicians who contribute significantly to SIGINT technological and cryptologic advances.

[Redacted]

NSA's formal INFOSEC relationship with CSE is based on a 1986 Memorandum of Agreement. The closeness of this relationship is illustrated through many programs:

[Redacted]

#### Relationship with Australia's Defence Signals Directorate (DSD) (U)

~~(TS-TKC-UO)~~ Also under the umbrella of UKUSA, the Melbourne Tripartite Conference of 1953 established SIGINT relationships among the U.S., Australia and New Zealand. The NSA-DSD relationship permits free exchange of SIGINT technical data and raw traffic

[Redacted]

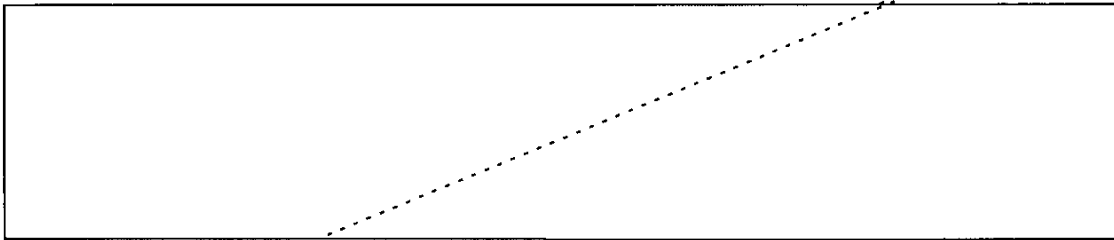
~~U.S. EYES ONLY~~

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~

~~TOP SECRET~~

~~TOP SECRET~~

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

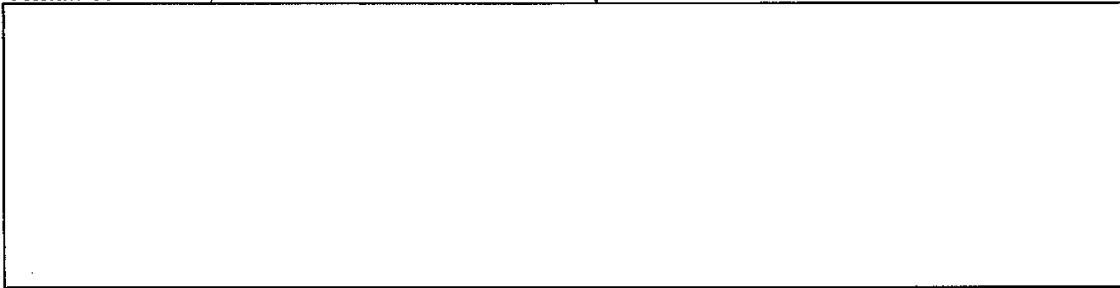


NSA's INFOSEC relationship with DSD is based on a 1970 agreement. Interoperability with U.S. Forces and protection of U.S. classified information are the primary reasons for releasing COMSEC to Australia. The U.S. is the primary provider of COMSEC equipment to the Government of Australia, and NSA supports U.S. equipment purchases by Australia with spare parts and training.

**Relationship with New Zealand's Government Communications Security Bureau (GCSB)**

(U)

~~(TS-CCO-UO)~~ Although the U.S.-NZ relationship was strained following New Zealand's 1985 prohibition of port visits by nuclear powered/armed vessels, the NSA-GCSB relationship remained virtually intact. NSA shares SIGINT of specific interest to New Zealand, and GCSB



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

~~U.S. EYES ONLY~~

~~HANDLE VIA TALENT KEYHOLE COMINT CONTROL SYSTEMS JOINTLY~~

~~TOP SECRET~~

~~SECRET~~

SECOND PARTIES

~~(S-CCO-NF)~~ The Second Parties (UK, Canada, Australia, and New Zealand) share a special status with respect to U.S. intelligence. The extremely close relationships will continue to expand in an evolutionary way; however, major expansion is unlikely since the exchanges are already all encompassing and we receive most of the intelligence these allies have to offer at their present level of resources. Increases in resources devoted to intelligence are unlikely in light of budgetary stringency and the diminishment of the Soviet threat.

~~(S-CCO-NF)~~ All of our Second Party relationships are generally thought to benefit the Second Party. U.S. goals for the future are to expand divisions of effort and to seek Second Party investment within their budget constraints in mutually beneficial intelligence projects that complement U.S. capabilities and take full advantage of Second Party access and geography.

~~(S-CCO-NF)~~ [Redacted]

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

~~NOFORN~~

~~HANDLE VIA COMINT CHANNELS ONLY~~  
~~SECRET~~



~~SECRET~~

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

UNITED KINGDOM

Current Basis of Relationship:

- Presidential authorization, 1945
- UKUSA COMINT Agreement of 1946; follow-on MOUs, DOEs, and policy statements.
- Wide-ranging and extensive exchange in all areas.

[Redacted]

Proposed Initiatives:

[Redacted]

Cost to the U.S.:

- No direct monetary cost.

[Redacted]

[Redacted]

Recommendations:

[Redacted]

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

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

~~HANDLE VIA TALENT KEYHOLE/COMINT CHANNELS JOINTLY~~

~~NOFORN~~

~~SECRET~~

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

~~SECRET~~

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

CANADA

**Current Basis of Relationship:**

- Established under the umbrella of the UKUSA COMINT Agreement of 1946 and tailored in the CANUSA Agreement of 1949.
- Wide-ranging and extensive exchanges

[Redacted]

[Redacted]

**Proposed Targets/Initiatives:**

[Redacted]

**Cost to the U.S.:**

- No direct monetary cost.

[Redacted]

**Recommendation:**

[Redacted]

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

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

~~HANDLE VIA COMINT CHANNELS ONLY~~  
~~SECRET~~

~~NOFORN~~

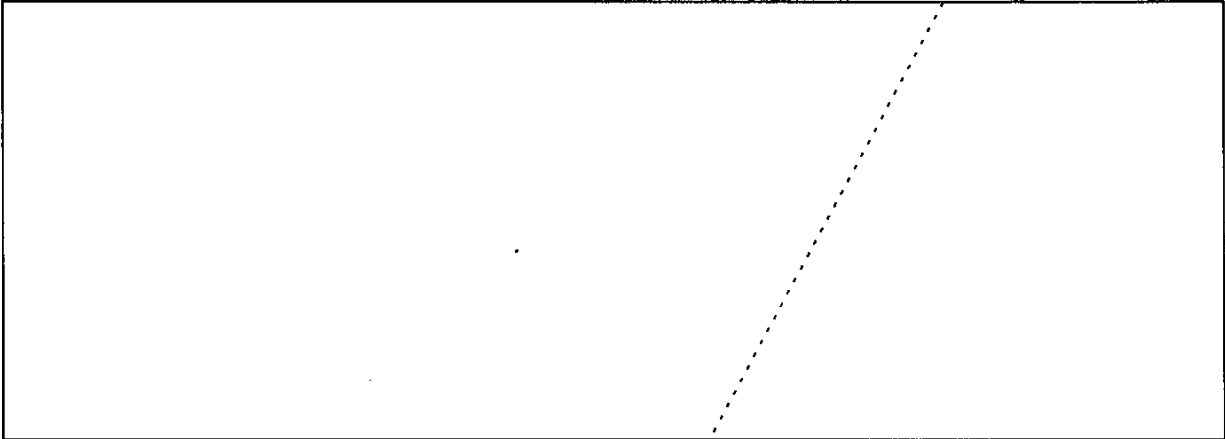
~~SECRET~~

(b) (1)  
(b) (3)-18 USC 793  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

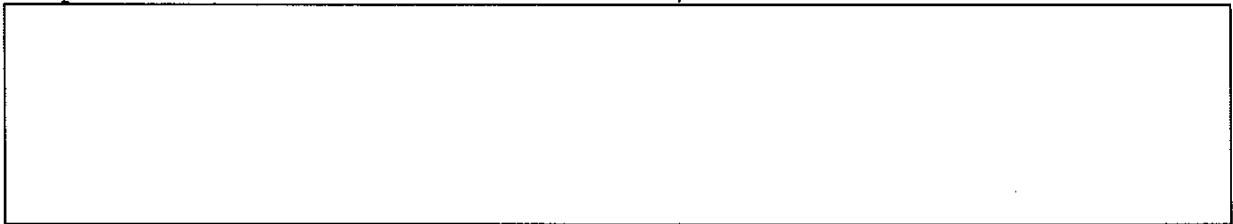
AUSTRALIA

Basis of Current Relationship:

- UKUSA Agreement of 1946, amplified by Melbourne Tripartite Conference of 1953.

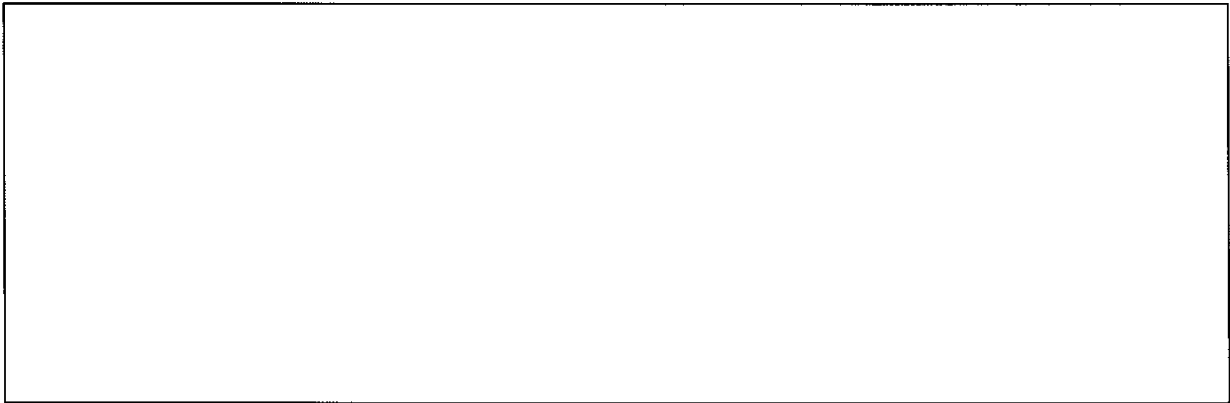


Proposed Initiatives:

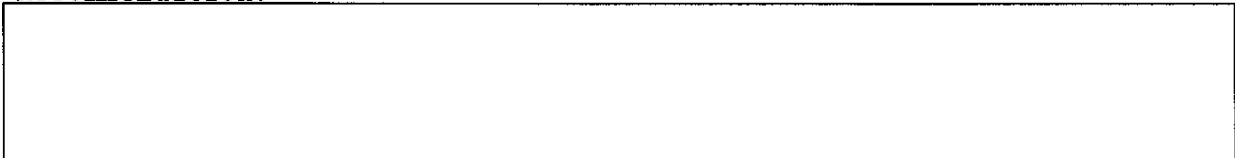


Cost to the U.S.:

- No direct monetary cost.



Recommendation:



~~HANDLE VIA TALENT KEYHOLE/COMINT CHANNELS JOINTLY~~

~~NOFORN~~

~~SECRET~~

(b) (1)  
(b) (3)-18 USC 793  
(b) (3)-50 USC 3024(i)  
(b) (3)-P.L. 86-36

~~SECRET~~

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

**NEW ZEALAND**

**Basis of Current Relationship:**

- UKUSA Agreement of 1946, amplified by Melbourne Tripartite Conference of 1953.

[Redacted]

**Proposed Initiatives:**

[Redacted]

**Cost to the U.S.:**

- No direct monetary costs.

[Redacted]

**Recommendation:**

[Redacted]

~~NOFORN~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~



NATIONAL SECURITY AGENCY  
CENTRAL SECURITY SERVICE  
NSA/CSS POLICY 1-13




Issue Date: 31 December 2014  
Revised:

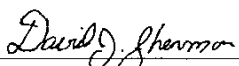
---

(U) SECOND PARTY INTEGREGES

(U) PURPOSE AND SCOPE

(U//~~FOUO~~) This policy assigns responsibilities and procedures for the establishment of *Second Party Integree* positions and the placement of Second Party Integrees, including personnel involved in military exchange programs, into NSA/CSS. This policy applies to *NSA/CSS Washington*, the *NSA/CSS Extended Enterprise*, and United States Signals Intelligence System tactical locations.

  
MICHAEL S. ROGERS  
Admiral, U.S. Navy  
Director, NSA/Chief, CSS

  
Endorsed by  
Associate Director for Policy

(U) DISTRIBUTION:  
DP09  
DJ1

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

NSA FOIA Case 100386 Page 00496

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Policy 1-13

Dated: 31 December 2014

(U) This Policy 1-13 supersedes NSA/CSS Policy 1-13 dated 16 August 2004.

(U) OPI: Foreign Affairs Directorate, DP, 963-5454s.

(U) No section of this document, regardless of classification, shall be released without approval from the Office of Corporate Policy (DJ1).

**(U) POLICY**

1. (U//~~FOUO~~) NSA/CSS shall support the integration of *Second Party* personnel into the NSA/CSS workforce throughout the *NSA/CSS Global Cryptologic Enterprise* when it is beneficial to the United States Cryptologic System mission, strengthens relationships with the Second Party nations, and is consistent with U.S. Government law, policy, strategy, and interests. The integration of Second Party personnel into the NSA/CSS workforce must be in compliance with Department of Defense Directive (DoDD) 5230.20, "Visits, Assignments, and Exchanges of Foreign Nationals" (Reference a).

2. (U//~~FOUO~~) Second Party Integrees shall not perform inherently governmental functions, which must remain the responsibility and within the purview of NSA/CSS Government employees.

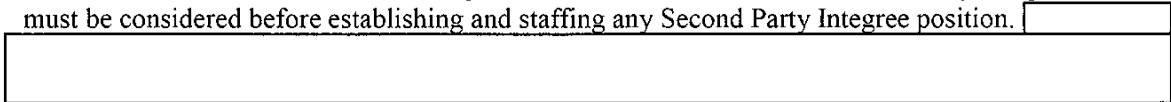
a. (U//~~FOUO~~) Second Party Integrees shall not be assigned responsibilities that involve direction of NSA/CSS decision-making processes or that include performing activities that require exercise of substantial direction in applying government authority, including binding NSA/CSS to take or not to take some action by contract, policy, or regulation; to make personnel decisions, including hiring functions; or to make financial/resource decisions. Second Party Integrees may not solely represent the corporate interests of NSA/CSS in internal or external meetings or conferences. While Second Party Integrees may occasionally be called upon to contribute unique expertise to such meetings or conferences, this is permissible only if the Second Party Integree is not asked to commit NSA/CSS resources or to represent NSA/CSS in a policymaking capacity.

b. (U//~~FOUO~~) Second Party Integrees may not perform information technology (IT) systems administrative functions or hold privileged user access on NSA/CSS IT systems, with the exception of local administrative privileges in direct support of mission requirements (i.e., a virtual machine or workstation the administrative access to which is expressly required for mission purposes). All Second Party accesses will comply with Intelligence Community Directive (ICD) Number 503, "Information Technology Systems Security Risk Management, Certification and Accreditation" (Reference b), DoDD 8500.01, "Cybersecurity" (Reference c), NSA/CSS Policy 6-3, "NSA/CSS Operational Information Systems Security Policy" (Reference d), and NSA/CSS Policy 6-20, "Second Party Access to NSA/CSS TS/SCI Classified Information Systems" (Reference e). Requests for exception to this paragraph shall be reviewed and endorsed by the Information System Security Officer (ISSO) prior to submission to the NSA/CSS Authorizing Official for decision.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

c. ~~(U//FOUO)~~ Second Party Integrees may be assigned to leadership positions; however, any supervisory responsibilities that are reserved by law or regulation to an officer or employee of the U.S. Government must be performed by the next higher level U.S. supervisor in the management or command chain. This prohibits the Second Party Integree leader from preparing human resource-related documents, including final performance evaluations, making pay decisions, making decisions regarding the employee's advancement to the next pay level or grade, making award decisions, or similar personnel actions, for any subordinate NSA/CSS employee. Second Party Integrees may, however, provide input to a U.S. Government employee's official supervisor concerning these matters. Additionally, access restrictions may prohibit a Second Party Integree in a leadership position from having full access to the specific details and scope of an NSA/CSS employee's most sensitive mission activities.

3. ~~(U//FOUO)~~ Information necessary for Second Party Integrees to perform their functions shall be shared unless specifically prohibited by NSA/CSS, Director of National Intelligence (DNI), DoD, or Committee on National Security Systems (CNSS) policy, applicable Executive Orders, or U.S. law. Security ramifications associated with Second Party Integrees must be considered before establishing and staffing any Second Party Integree position.



4. (U) Organizations wishing to establish and staff new Second Party Integree positions shall follow the procedures detailed below.

**(U) PROCEDURES**

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

5. ~~(U//FOUO)~~ Requirements for Second Party Integree positions will be identified within NSA/CSS Directorates, Associate Directorates, the NSA/CSS Chief of Staff organization, or NSA/CSS Extended Enterprise elements. This policy permits informal exchanges between NSA/CSS and Second Party organizations to identify and define those requirements.

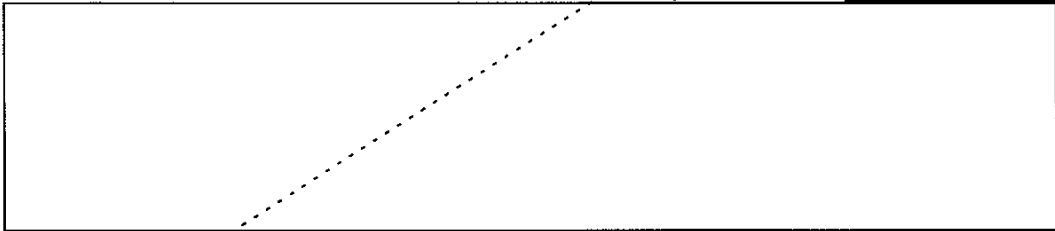
6. ~~(U//FOUO)~~ The gaining organization wishing to establish, extend, or reallocate an integrated position will prepare, coordinate, and formally track the necessary documentation through the Second Party Affairs Office of the Signals Intelligence (SIGINT) Operations Group (DPI), Foreign Affairs Directorate (FAD), and the Associate Directorate for Security & Counterintelligence (ADS&CI) to the appropriate Director, Deputy Director, Associate Director, or NSA/CSS Chief of Staff. Extended Enterprise elements will work through the appropriate governing Headquarters Directorate for review and approval. For SID, the approval authority is in accordance with the SID Delegation of Approval Authorities matrix. The approved package will be returned to FAD for final review and coordination with the affected Second Party Liaison Office and subsequent administration of the accountability processes.

7. ~~(U//FOUO)~~ The appropriate Director, Associate Director, the NSA/CSS Chief of Staff, or a designee may approve waivers to this policy when necessary to effect rapid reallocation of Second Party Integree resources in response to urgent mission requirements.

8. (U) General criteria for establishing and staffing a new Second Party Integree position.

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

a. (U//~~FOUO~~) NSA/CSS organizations establishing a new Second Party Integree position must first clearly identify and carefully consider the specific mission and associated data needs. Raw SIGINT data, intelligence products, or the immediate capability to produce them shall be shared with Integrees only in accordance with DoD, Intelligence Community (IC), NSA/CSS, and SID policy, as appropriate.



In addition, a Non-Disclosure Agreement (NDA) shall be executed with the Second Party Integree before release of any PROPIN data.

b. (U//~~FOUO~~) There is no minimum assignment length required for a Second Party Integree to obtain an NSANet account. Further, there is no minimum assignment length required for a Second Party Integree to be eligible for access to raw SIGINT data.

c. (U//~~FOUO~~) Second Party personnel who are solely attending NSA/CSS sponsored training are exempt from this policy. However, if access to NSA/CSS networks is a required part of their training, Second Party personnel shall adhere to NSA/CSS Policy 6-20 (Reference e).

d. (U//~~FOUO~~) Security considerations regarding the work-related activities of Second Party Integrees and associated access requirements shall be analyzed, and associated risks mitigated, by the operational element and subject to ADS&CI review and approval, to ensure compliance with information systems, physical, and personnel security policies before establishing and staffing any position.

e. (U//~~FOUO~~) Prior to establishing and staffing a proposed Second Party Integree position, all requirements shall be fully coordinated with the appropriate NSA/CSS offices. New Second Party Integree positions or Second Party Integree assignment extensions must receive prior approval by the head of the organization to which the Integree will be assigned, or by those having specifically delegated approval authority. Second Party Integree reassignment actions shall be coordinated through both the gaining and the losing approval authorities; disagreements will be resolved at the lowest appropriate levels. If the proposed Second Party Integree position will require rotational assignments, such as is required for many developmental programs (e.g., Cryptologic Mathematician Program, Language Analyst Training Program, etc.), each rotational assignment shall be handled as a Second Party Integree reassignment. All appropriate approvals and applicable documentations must be obtained at least 90 days prior (or less,



if agreed to by the gaining and losing approval authorities) to the Second Party Integree beginning the new rotational assignment.

9. ~~(U//FOUO)~~ In cases where a Second Party Integree will require interaction with any U.S. Government contractor, the U.S. Government contractor will be required to comply with U.S. laws, rules, and regulations, including those governing exports (e.g., the Arms Export Control Act and the International Traffic-In-Arms Regulations (ITAR), 22 CFR 120-130 (Reference f)). The Office of Export Control Policy (DJ3) is the signatory and authority for exemptions. DJ3 identifies the process required for contractors to interact with Second Party Integrees (Reference g).

10. (U) The Office of the General Counsel will advise on any questions regarding whether the integration of Second Party personnel into the NSA/CSS workforce or Second Party use of NSA/CSS capabilities is consistent with the U.S. laws and procedures that govern NSA/CSS activities.

**(U) RESPONSIBILITIES**

11. ~~(U//FOUO)~~ Directors, Associate Directors, the NSA/CSS Chief of Staff, and the Extended Enterprise Commanders/Chiefs shall:

a. ~~(U//FOUO)~~ Identify requirements for Second Party Integree positions and approve assignments, extensions, and reassignments within their respective organizations;

b. ~~(U//FOUO)~~ Document Second Party Integree requirements for the Second Party Affairs Office (DP1). This documentation shall include the following:

1) ~~(U//FOUO)~~ A justification stating why establishing a particular Second Party Integree position is necessary or beneficial to either the U.S. cryptologic mission or the Second Party relationship;

2) ~~(U//FOUO)~~ A description of the specific duties the Second Party Integree will be performing;

3) (U) Affirmation that the level of intelligence and information assurance sharing is consistent with current operational requirements and a statement that lists the security clearances required for the position;

~~(U//FOUO)~~ 4) (U) A statement of information system connectivity or access requirements, including access to [redacted] databases or datasets and access to raw SIGINT data; Integrees into SID will follow SID Management Directive 427, "Access to Data for Second Party Personnel Engaged in SIGINT Production" (Reference h);

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

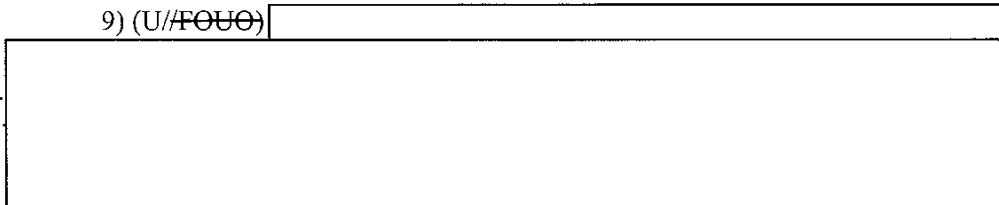
5) (U//~~FOUO~~) A description of the specific procedures that will be instituted within the assigned operational element to prevent the inadvertent disclosure of NOFORN information, information that is releasable to a community of which the Second Party Integree is not a member (for example, REL US/UK information for a Canadian Integree) (hereafter referred to as non-releasable information), or NSA/CSS Special Access Program material (Reference i) unless separate approval has been granted per paragraph 3;

6) (U//~~FOUO~~) Agreement regarding nondisclosure of proprietary or "commercial-in-confidence" information which would otherwise be required or available during a Second Party Integree's tenure. Non-disclosure will be managed within the organization to which the Integree is assigned and an acceptable plan must be in place to prevent the unauthorized and unintended release of PROPIN;

7) (U) Requirements for special training needed by the Second Party Integree, including mandatory intelligence oversight training, other training required of personnel working under DIRNSA/CHCSS SIGINT authority, or National Cryptologic School courses;

8) (U//~~FOUO~~) Assurance that the Second Party parent organization, through the Second Party Liaison Office, maintains security oversight and provides guidance for their assigned Second Party Integree personnel, in coordination with FAD, ADS&CI, and the involved OPI(s);

9) (U//~~FOUO~~)



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

10) (U//~~FOUO~~) An acknowledgement of specific, gaining organization responsibilities with regard to the Integree's operational and personnel management needs. The gaining organization accepts responsibility for performing active oversight of the Integree's SIGINT or information assurance (IA) activities. This includes, at a minimum, that the Integree's U.S. supervisor will have an Annual Contribution Evaluation with objectives that require the supervisor to:

a) (U//~~FOUO~~) Keep records of data access, especially non-releasable data; and

b) (U//~~FOUO~~) Perform audits of requisite databases accesses.

c. (U//~~FOUO~~) Coordinate with ADS&CI, the Technology Directorate, and the relevant Oversight and Compliance Organization to assess potential security vulnerabilities for integrating Second Party personnel into a specific operational element;

d. (U//~~FOUO~~) Review the qualifications of, and approve or disapprove, candidates who are nominated to fill Second Party Integree positions. Forward Second Party Integree selections or non-selections to the Second Party Affairs Office (DP1);

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

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

f. (U//~~FOUO~~) Coordinate with the Information Assurance Directorate (IAD) when a Second Party Integree has an Office of Primary Interest (OPI)-approved requirement for access to United States Information Security data, including, but not limited to, IA threat and vulnerability information, U.S. cryptographic algorithms, IA techniques, or U.S. computer security information;

g. (U//~~FOUO~~) Coordinate with the appropriate Information Systems Security Officer and/or Information Systems Security Manager so that appropriate security certification and accreditation documents, risk assessments, and security controls (if required) can be updated before the Second Party Integree arrives for duty and is given access to an information system, in accordance with NSA/CSS Policy 6-20, "Second Party Access to NSA/CSS TS/SCI Classified Information Systems" (Reference e); and

h. (U//~~FOUO~~) Advise the FAD Second Party Affairs Office of any proposed changes in the status of Second Party Integree positions, including rotation, extension, and/or replacement of specific personnel, at least 90 days in advance of the proposed change whenever possible.

12. (U) The Foreign Affairs Director shall:

a. (U//~~FOUO~~) Review all requests for establishing, extending, or reassigning Second Party Integree positions. This includes verifying and endorsing conformance with existing policy and procedures;

b. (U//~~FOUO~~) Coordinate with Second Party Liaison Offices to establish Second Party Integree positions and/or personnel status changes;

c. (U//~~FOUO~~) Advise the requesting operational element of candidates nominated to fill Second Party Integree positions and the dates of availability. Solicit operational element approval(s);

d. (U) Notify the affected Second Party Liaison Office of approvals and

disapprovals of Second Party Integree positions;

e. (U//~~FOUO~~) Advise appropriate organizations when all necessary administrative, security, and personnel actions have been addressed by the responsible offices prior to the arrival or transfer of an individual Second Party Integree;

f. (U//~~FOUO~~) Maintain a current corporate record of all Second Party Integrees at NSA and the Extended Enterprise, including names, assigned organization, and length of tour; and

g. (U//~~FOUO~~) Ensure that the Second Party parent organization, through the Second Party Liaison Office, provides ADS&CI with clearance certification and relevant background information on a proposed Integree (at a minimum, name, date and place of birth, date of last security background investigation or reinvestigation, citizenship, and citizenship of spouse or "significant other" partner cohabitating with the Integree);

13. (U) The Associate Director for Security and Counterintelligence shall:

a. (U//~~FOUO~~) Review and assess the personnel and physical security vulnerabilities of integrating Second Party personnel into specific NSA/CSS operational element positions and, if appropriate, provide recommendations to mitigate associated risks;

b. (U//~~FOUO~~) Establish individual security records on each Second Party Integree consisting of basic identification, clearance certification status, and current accesses, excluding personal data associated with background/vetting investigations and updates, that remain under the purview of an Integree's home agency;

c. (U//~~FOUO~~) Certify and maintain applicable identification, clearance, and eligibility for access information for all Second Party Integrees;

d. (U) Administer and maintain records of NSA/CSS "Special Access" information granted to Second Party Integrees in accordance with Reference i; and

e. (U) Issue each Second Party Integree the appropriate access token (badge) required for access to NSA/CSS-controlled campuses and buildings in accordance with NSA/CSS Policy 5-7, "NSA/CSS Badge Identification System" (Reference j).

14. (U) The Technology Director, as the NSA/CSS Chief Information Officer, and the NSA/CSS Chief Information Security Officer (CISO) shall:

a. (U//~~FOUO~~) Review and assess the information systems security ramifications of integrating or retaining Second Party personnel within specific NSA/CSS operational element positions;

b. (U//~~FOUO~~) Provide information systems security guidance, in accordance with the requirements of References a, b, and c, to organizations requesting Second Party access to NSA/CSS computer systems or networks and company PROPIN; and

c. (U//~~FOUO~~) Implement and oversee the technical infrastructure that supports digital identity (i.e. Cryptologic Agencies Domain, Reference e) for Second Party Integrees, enabling appropriate identification, authorization, and audit capability for the NSA/CSS TOP SECRET SCI network.

**(U) REFERENCES**

15. (U) References:

a. (U) DoDD 5230.20, "Visits and Assignments of Foreign Nationals," dated 22 June 2005.

b. (U) ICD 503, "Information Technology Systems Security Risk Management, Certification and Accreditation," dated 15 September 2008. (Intelink)

c. (U) DoDI 8500.01, "Cybersecurity," dated 14 March 2014.

d. (U) NSA/CSS Policy 6-3, "Information Technology Security Authorization Using the Risk Management Framework," dated 7 March 2014.

e. (U) NSA/CSS Policy 6-20, "Second Party Access to NSA/CSS TS/SCI Classified Information Systems," dated 31 March 2014.

f. (U) International Traffic in Arms Regulations (ITAR), 22 CFR 120-130, dated 29 August 2005.

g. (U) NSA/CSS Policy 1-7, "Technology Security Program," dated 24 December 2013.

h. (U) SID Management Directive 427, "Access to Classified U.S. Intelligence Information for Second Party Personnel," dated 28 December 2013.

i. (U) NSA/CSS Policy 1-41, "Programs for the Protection of Especially Sensitive Classified Information," dated 7 March 2013 and revised 6 February 2014.

j. (U) NSA/CSS Policy 5-7, "NSA/CSS Badge Identification System," dated 26 October 2007.

k. (U) Executive Order 12333, "United States Intelligence Activities," as amended.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Policy 1-13

Dated: 31 December 2014

**(U) DEFINITIONS**

16. (U//~~FOUO~~) Non-releasable Information – NOFORN information or information that is releasable to a community of which the Second Party Integree is not a member (for example, REL US/UK information for a Canadian Integree).

17. (U) NSA/CSS Global Cryptologic Enterprise – NSA/CSS worldwide personnel, systems, and facilities:

a. (U) NSA/CSS Headquarters: Primary location of the NSA/CSS Senior Leadership Team.

b. (U) NSA/CSS Washington (NSAW): NSA/CSS facilities at the Fort Meade, FANX, and associated campuses [Finksburg, Kent Island, and all leased facilities in the Baltimore/Washington metropolitan area].

c. (U) NSA/CSS Extended Enterprise (Field): NSA/CSS personnel, systems, and facilities at locations other than NSAW. (Source: Corporate Glossary)

18. (U//~~FOUO~~) Raw SIGINT Data – Any SIGINT data acquired either as a result of search and development or targeted collection operations against a particular foreign intelligence target before the information has been minimized and evaluated for foreign intelligence purposes. (Source: Corporate Glossary)

19. (U//~~FOUO~~) Second Party – Any of the four countries with which the U.S. Government maintains SIGINT and IA relationships, namely the United Kingdom, Canada, Australia, and New Zealand.

20. (U//~~FOUO~~) Second Party Integrees – Second Party personnel integrated into an NSA/CSS or United States Cryptologic System element who, when integrated into an NSA/CSS environment, are working solely under the direction and operational control of the DIRNSA/CHCSS to conduct cryptologic or information assurance activities that support NSA/CSS mission in accordance with NSA/CSS authorities, rules, and regulations. Integrees may be civilian or military Second Party SIGINT or IA personnel but may not be contractors. Equivalent to the term Foreign Exchange Personnel: an individual from one of the Second Party cryptologic entities assigned to work for NSA/CSS under DIRNSA/CHCSS authorities. Duties associated with an Integree's position shall be performed in support of the NSA/CSS mission and in compliance with Executive Order 12333, "United States Intelligence Activities," as amended (Reference k).

21. (U//~~FOUO~~) Second Party Liaison – An individual representing one of the Second Party nations' SIGINT or IA counterpart organizations at NSA/CSS. Duties associated with this position will be performed primarily in support of the counterpart organization.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

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

NSA/CSS DIR. NO. 21-3  
DATE: 26 November 1990



NSA/CSS DIRECTIVE  
SECOND PARTY INTEGREES (U)

SECTION

PURPOSE..... I  
 DEFINITIONS.....II  
 POLICY.....III  
 RESPONSIBILITIES.....IV  
 PROCEDURES.....V

SECTION I - PURPOSE AND APPLICABILITY

1. This directive establishes policy, assigns responsibilities and prescribes procedures for the establishment of Second Party integree positions within the NSA/CSS. This directive is applicable to all cryptologic sites and facilities located within CONUS or overseas and includes those sites or facilities operated/managed either directly by the NSA/CSS or the Service Cryptologic Elements (SCEs).

SECTION II - DEFINITIONS

2. Second Party: That term applied either individually or collectively to the following nations with whom the NSA/CSS maintains special SIGINT and INFOSEC exchange relationships:

- The United Kingdom
- Canada
- Australia
- New Zealand

3. Second Party Integree Position: A position established by NSA/CSS (to include CONUS or overseas cryptologic facilities) which will be filled on a permanent change of station (PCS)

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

OPI: DDPP ( [redacted] ) Q41, 963-3086

Approved for Release  
by NSA on 09-20-2018,  
FOIA Litigation Case  
#100386 Page 00506

NSA/CSS DIRECTIVE NO. 21-3

basis by an individual representing one of the Second Party nations. Duties associated with this position will be performed in furtherance of the mission of NSA/CSS.

SECTION III - POLICY

4. The integration of Second Party personnel into the NSA/CSS work force is supported when it is beneficial to the U.S. SIGINT or INFOSEC mission, or its SIGINT or INFOSEC relationships with the Second Party Nations identified in paragraph 2., above.

5. Security ramifications to include possible exposure to special operations or compartments, NOFORN, industrial proprietary or any other information not releasable to Second Parties, must be considered prior to the establishment and staffing of any Second Party integree positions.

6. All requirements for Second Party integrees will be fully coordinated with appropriate Second Party SIGINT or INFOSEC authorities and approved by the affected Key Component Chief (or the Chief of a CONUS or overseas cryptologic site or facility) prior to the establishment and staffing of the proposed positions.

7. Second Party integrees will not be placed in positions in which they have a direct effect upon the NSA/CSS decision-making process, to include both contractual and policy deliberations. Under no circumstances should they be placed in positions whereby they are solely responsible for addressing such issues, nor represent Agency interests in external meetings or conferences.

8. The processing, staffing and assignment of Second Party personnel to CONUS or overseas cryptologic sites or facilities will be handled in the same manner as Second Party personnel integrated into NSA/CSS Headquarters elements.

9. The temporary assignment of Second Party personnel for on-the-job or classroom training (for a period not to exceed six months) is not subject to the processing and approval requirements of this Directive. Host organizations, however, must ensure that security and administrative steps are taken to preclude inadvertent disclosure of U.S. or NSA/CSS-only information for the duration of the training period.



NSA/CSS DIRECTIVE NO. 21-3

SECTION IV - RESPONSIBILITIES

10. The Chiefs of Key Components and Chiefs of CONUS or overseas cryptologic sites or facilities will:

a. Identify requirements for Second Party integree positions and assignments within their respective organizations.

b. Prepare written documentation of Second Party integree requirements. This documentation will include the following information:

(1) A justification as to why the establishment of the position is necessary or important to either the U.S. SIGINT or INFOSEC mission or the Second Party relationship.

(2) A description of the specific duties the Second Party integree will be performing.

(3) The specific procedures that will be instituted within the assigned organization to preclude the inadvertent disclosure of U.S.-only information or Special Activities Programs.

c. Coordinate with the Deputy Director for Operations (DDO), Special Activities Office (P05/SAO) regarding special access requirements, and with the Deputy Director for Administration (DDA), Security (M5), to assess any special security considerations, e.g. key control, lock installations, access control to ADP systems, etc., that may be needed to provide adequate safeguards to preclude the inadvertent disclosure of sensitive U.S.-only information or other proprietary equities.

d. Forward Second Party integree position requests to the Deputy Director for Plans and Policy (DDPP) for review (verification of conformance with existing policy) and approval.

e. Review the qualifications of and approve candidates who are nominated to fill Second Party integree positions.

f. Advise the DDPP of any changes in the status of Second Party integree positions to include rotation and replacement of specific personnel.

NSA/CSS DIRECTIVE NO. 21-3

g. Establish procedures for the non-disclosure of proprietary or "commercial-in-confidence" information which is required during an integree's tenure.

h. Coordinate with the NSA/CSS SCSM (Senior Computer Security Manager) and the Information Systems Security International Relations, Policy and Doctrine Organization (S1) when an integree or trainee has a requirement for access to U.S. Information Systems Security information, including but not limited to INFOSEC threat and vulnerability information, U.S. cryptographic algorithms or INFOSEC techniques, or U.S. computer security information.

11. The Deputy Director for Plans and Policy (DDPP) will:

a. Review and approve all requests for establishment of Second Party integree positions to verify and endorse conformance of the requests with existing policy.

b. Coordinate with the Second Party liaison offices to staff these positions.

c. Solicit the approval of requesting organizations for candidates nominated to fill Second Party integree positions.

d. Maintain a record of all Second Party integrees to include names, assigned elements, length of tour, etc. (Q32).

e. Obtain, from the Second Party parent organization, a certification of the clearances/accesses of proposed integrees, as well as relevant background information on the proposed integree (to include at a minimum name, date and place of birth, date of last Security Background Investigation or reinvestigation, citizenship, and citizenship of spouse). The Office of Foreign Relations (Q3) will provide this information to M5 and P05/SAO and will advise those organizations of any changes in the status of integrees which would affect their clearances/access certifications.

12. The Deputy Director for Administration (DDA) will:

a. Provide advice and assistance regarding physical and personnel security policies and procedures as they may relate to integrating Second Party personnel into specific NSA/CSS organizations in CONUS or overseas.

NSA/CSS DIRECTIVE NO. 21-3

b. Establish and maintain a data base of clearance and security background information initially provided and kept current by Q3 for all Second Party integrees.

c. Review security background data provided by Q3 on nominated Second Party integrees, and provide endorsements to Q3 prior to Agency acceptance of the integree for assignment.

13. The Deputy Director for Operations (DDO) will administer and maintain records of accesses to NSA/CSS special access programs by all Second Party integrees (P05/SAO).

14. The Deputy Director for Telecommunication and Computer Services, (DDT), under the auspices of the Office of Operational Computer Security (T03), will:

a. Review and assess the computer security ramifications of integrating Second Party personnel into specific NSA/CSS positions.

b. Provide, in accordance with the requirements of DCID 1/16 (Security Policy for Uniform Protection of Intelligence Processed in Automated Information Systems and Networks), computer security guidance to organizations requesting Second Party access to NSA/CSS computer systems or networks.

SECTION V - PROCEDURES

15. Requirements for Second Party integrees will be identified within the operational elements of the Key Components or CONUS or overseas cryptologic sites or facilities. This regulation does not preclude informal exchanges between NSA/CSS and Second Party operational elements for purposes of identifying and defining those requirements.

16. The operational element wishing to establish an integrated position will prepare and forward the necessary paperwork to their Key Component Chief (or Chief of CONUS or overseas cryptologic site or facility) for review and approval.

17. The Chiefs of Key Components or Chiefs of CONUS or overseas cryptologic sites or facilities will review, approve and forward Second Party integree requirements to the Deputy Director for Plans and Policy.

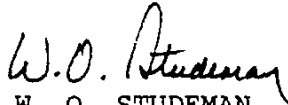
NSA/CSS DIRECTIVE NO. 21-3

18. Q3, in coordination with the Office of Policy (Q4), will perform necessary policy reviews and prepare an appropriate recommendation for the DDPP.

19. Subject to DDPP endorsement, Q3 will coordinate with the Second Party liaison offices to begin the staffing process.

20. Q3 will advise the requesting organization of candidates nominated to fill Second Party integrated positions and reporting dates and solicit their approval to proceed with follow-on staffing actions.

21. Q3, upon approval of the Key Component Chief or the Chief of a CONUS or overseas cryptologic site or facility, will advise M5 and P05/SAO of the individual selected to fill a Second Party integrated position. This will ensure that all necessary administrative, security and personnel actions are adequately addressed prior to the arrival of that individual.



W. O. STUDEMAN  
Vice Admiral, U.S. Navy  
Director

---

DISTRIBUTION II

Plus: Q32 (20 copies)  
Q41 (20 copies)  
F92 (VRD)

~~SECRET~~  
Assistant Deputy Director  
for  
Plans and Policy

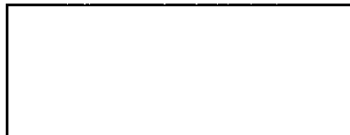
28 SEP 1984

TO: DISTRIBUTION

SUBJECT: UKUSA Joint Goals and Objectives

1. ~~(S-CCO-NOFORN)~~ GCHQ has written a statement on the relationship between UKUSA Joint Goals and Objectives and actual planning taking place (Encl. 1). Note that after each UKUSA Goal and Objective, GCHQ has identified "Relevant Plans and Actions" pursuant to the achievement of the G & O. Because we envision the statement will be useful to NSA in pursuing our Second Party strategy, request your review and comments NLT 12 October 1984.

2. (U) Also provided for your information is a recent letter to the Head of the P Staff, GCHQ, concerning a proposed tracking mechanism for evaluating progress made on UKUSA Joint G&Os (Encl. 2).



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

Encls:  
a/s

~~Classified By: N31 1000000000~~  
~~Declassify On: OADR Determination Required~~

~~NOT RELEASABLE TO FOREIGN NATIONALS~~

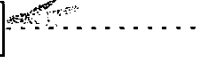
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

DISTRIBUTION:

DDO  
DDC  
DDR  
DDT  
ADC

Q32 (Miss



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

Doc ID: 6636914

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

Attachment to P/0881PP/8000/5

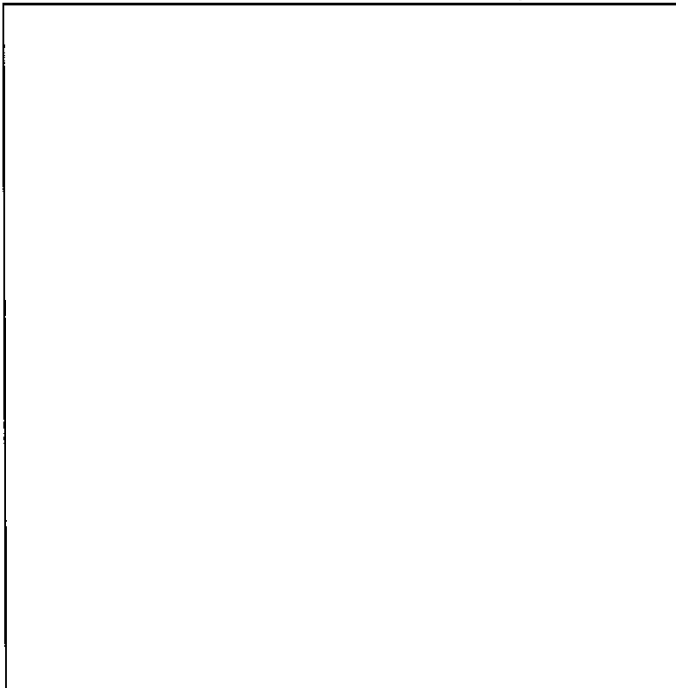
GOAL I

A cooperative relationship which maximises the jointness of UKUSA current and future efforts while preserving the essential national characteristics.

OBJECTIVE A.



RELEVANT PLANS AND ACTIONS



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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~



~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL I

A cooperative relationship which maximises the jointness of UKUSA current and future efforts while preserving the essential national characteristics.

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

OBJECTIVE B

[Redacted]

RELEVANT PLANS AND ACTIONS

- a.
- b.
- c.
- d.
- e.
- f.
- g.
- h.
- i.

[Redacted]

[Redacted]

(b) (1)  
(b) (3) - 18 USC 793  
(b) (3) - 50 USC 3024(i)  
(b) (3) - P.L. 86-36

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

3

Attachment to P/0881PP/8000/5

GOAL I

A cooperative relationship which maximises the jointness of UKUSA current and future efforts while preserving the essential national characteristics.

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

OBJECTIVE C

[Redacted]

RELEVANT PLANS AND ACTIONS

- a.
- b.
- c.
- d.
- e.
- f.
- g.
- h.
- i.
- j.

(b) (1)  
(b) (3) - 18 USC 793  
(b) (3) - 50 USC 3024(i)  
(b) (3) - P.L. 86-36

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL II

A SIGINT capability which ensures strategic warning, limits surprise and develops timely information on international activities inimical to the interests of UKUSA.

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

OBJECTIVE A

[Redacted]

RELEVANT PLANS AND ACTIONS

Much of the GCHQ effort is directed towards this objective. Measures on specific threats include:

- a.
  - b.
  - c.
  - d.
  - e.
  - f.
  - g.
  - h.
  - i.
- [Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

5

Attachment to P/0881PP/8000/5



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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL II

A SIGINT capability which ensures strategic warning, limits surprise and develops timely information on international activities inimical to the interests of UKUSA.

OBJECTIVE B

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

[Redacted]

RELEVANT PLANS AND ACTIONS

- a.
- b.
- c.
- d.

[Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL II

A SIGINT capability which ensures strategic warning, limits surprise and develops timely information on international activities inimical to the interests of UKUSA.

OBJECTIVE C

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

[Redacted]

RELEVANT PLANS AND ACTIONS

- a.
- b.
- c.
- d.
- e.
- f.

[Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GCAL III

SIGINT support responsive to UK, US and Allied national-level and localised (such as tactical) requirements in which all users have confidence.

OBJECTIVE A

[Redacted]

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

RELEVANT PLANS AND ACTIONS

- a. [Redacted]
- b. [Redacted]
- c. [Redacted]
- d. [Redacted]
- e. [Redacted]
- f. [Redacted]
- g. [Redacted]
- h. [Redacted]
- i. [Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL III

SIGINT support responsive to UK, US and Allied national-level and localised (such as tactical) requirements in which all users have confidence.

OBJECTIVE B

[Redacted]

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

RELEVANT PLANS AND ACTIONS

- a.
  - b.
  - c.
  - d.
  - e.
  - f.
  - g.
  - h.
  - i.
- [Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~



~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

10

Attachment to P/C881PP/8000/5

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

GOAL III

SIGINT support responsive to UK, US and Allied national-level and localised (such as tactical) requirements in which all users have confidence.

OBJECTIVE C.

[Redacted]

RELEVANT PLANS AND ACTIONS

- a.
- b.
- c.
- d.
- e.

[Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

11

Attachment to P/0881PP/8000/5

GOAL III

SIGINT support responsive to UK, US and Allied national-level and localised (such as tactical) requirements in which all users have confidence.

OBJECTIVE D

[Redacted]

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

RELEVANT PLANS AND ACTIONS

- a. [Redacted]
- b. [Redacted]
- c. [Redacted]
- d. [Redacted]
- e. [Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

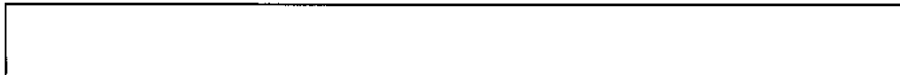
12

Attachment to P/0881PP/8000/5

GOAL III

SIGINT support responsive to UK, US and Allied national-level and localised (such as tactical) requirements in which all users have confidence.

OBJECTIVE E



RELEVANT PLANS AND ACTIONS

This subject is included in the GCRQ/NSA Planning Conference.

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

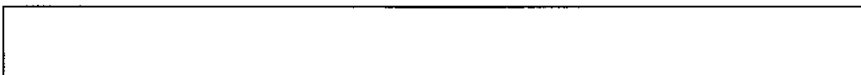
13

Attachment to P/0881PP/8000/5

GOAL III

SIGINT support responsive to UK, US and Allied national-level and localised (such as tactical) requirements in which all users have confidence.

OBJECTIVE F



RELEVANT PLANS AND ACTIONS

This subject is included in the GCHQ/NSA Planning Conference and needs to be closely geared to Objective B.

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

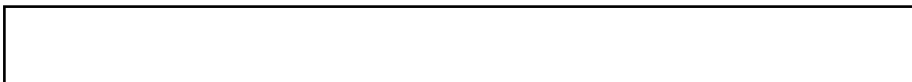
14

Attachment to P/0881PP/8000/5

GOAL III

SIGINT support responsive to UK, US and Allied national-level and localised (such as tactical) requirements in which all users have confidence.

OBJECTIVE G



RELEVANT PLANS AND ACTIONS

This subject is included in the GCHQ/NSA Planning Conference.

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

15 Attachment to P/0881PP/8000/S

GOAL IV

A flexible and efficient UKUSA collection and processing capability able to respond to changes in requirement and target.

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

OBJECTIVE A

[Redacted]

RELEVANT PLANS AND ACTIONS

- a.
- b.
- c.
- d.
- e.
- f.
- g.

(b) (1)  
(b) (3)-18 USC 793  
(b) (3)-50 USC 3024 (i)  
(b) (3)-P.L. 86-36

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL IV

A flexible and efficient UKUSA collection and processing capability able to respond to changes in requirement and target.

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

OBJECTIVE B

[Redacted]

RELEVANT PLANS AND ACTIONS

- a.
- b.
- c.
- d.
- e.

[Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
HANDLE VIA COMINT CHANNELS ONLY

GOAL IV

A flexible and efficient UKUSA collection and processing capability able to respond to changes in requirement and target.

OBJECTIVE C

[Redacted]

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

RELEVANT PLANS AND ACTIONS

- a. [Redacted]
- b. [Redacted]
- c. [Redacted]
- d. [Redacted]
- e. [Redacted]
- f. [Redacted]
- g. [Redacted]

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

~~TOP SECRET~~  
HANDLE VIA COMINT CHANNELS ONLY



~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNEL ONLY~~

GOAL IV

A flexible and efficient UKUSA collection and processing capability able to respond to changes in requirement and target.

OBJECTIVE D

[Redacted]

[Redacted]

RELEVANT PLANS AND ACTIONS

a. This subject is covered by the GCRQ/NSA Planning Conference.

b. [Redacted]  
c. [Redacted]  
d. [Redacted]  
e. [Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNEL ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL IV

A flexible and efficient UXUSA collection and processing capability able to respond to changes in requirement and target.

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

OBJECTIVE E

[Redacted]

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

RELEVANT PLANS AND ACTIONS

- a.
  - b.
  - c.
  - d.
  - e.
  - f.
  - g.
  - h.
  - i.
- [Redacted]

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL IV

A flexible and efficient UKUSA collection and processing capability able to respond to changes in requirement and target.

OBJECTIVE F

[Redacted]

RELEVANT PLANS AND ACTIONS

- a.
- b.
- c.
- d.
- e.
- f.
- g.
- h.

[Redacted]

(b) (1)  
(b) (3)-18 USC 793  
(b) (3)-50 USC 3024 (1)  
(b) (3)-P.L. 86-36

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

21 Attachment to P/0881PP/8000/5

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

GOAL V

Readability upon demand of a higher proportion than in the early 1980s of all foreign cryptographic systems and of certain foreign computer systems.

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

OBJECTIVE A

[Redacted]

RELEVANT PLANS AND ACTIONS

- a.
- b.
- c.
- d.
- e.

[Redacted]

[Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL V

Readability upon demand of a higher proportion than in the early 1980s of all foreign cryptographic systems and of certain foreign computer systems.

OBJECTIVE B

[Redacted]

RELEVANT PLANS AND ACTION

a. Maintain contact on potential opportunities in [Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL V

Readability upon demand of a higher proportion than in the early 1980s of all foreign cryptographic systems and of certain foreign computer systems.

OBJECTIVE C

[Redacted]

RELEVANT PLANS AND ACTIONS

- a.
- b.
- c.
- d.
- e.

[Redacted]

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

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL V

Readability upon demand of a higher proportion than in the early 1980s of all foreign cryptographic systems and of certain foreign computer systems.

OBJECTIVE D

[Redacted]

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

RELEVANT PLANS AND ACTIONS

Working exchanges between

[Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL VI .

A UKUSA SIGINT information dissemination process which meets customer requirements while maintaining production and processing security and the need to know principle.

OBJECTIVE A

[Redacted]

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

RELEVANT PLANS AND ACTIONS

- a.
- b.
- c.
- d.
- e.

[Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~



~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

26 Attachment to P/0881PP/8000/5

GOAL VI

A UKUSA SIGINT information dissemination process which meets customer requirements while maintaining production and processing security and the need to know principle.

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

OBJECTIVE B

[Redacted]

RELEVANT PLANS AND ACTIONS

- a.
- b.
- c.
- d.
- e.
- f.

[Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL VII

Third Party SIGINT relationships which optimise their contribution to UKUSA.

OBJECTIVE A

[Redacted]

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

RELEVANT PLANS AND ACTIONS

- a. [Redacted]
- b. [Redacted]
- c. [Redacted]
- d. [Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

28 Attachment to P/0881PP/8000/5

GOAL VII

Third Party SIGINT relationships which optimise their contribution to UKUSA.

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

OBJECTIVE B

[Redacted]

RELEVANT PLANS AND ACTIONS

- a.
- b.

[Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL VII

Third Party SIGINT relationships which optimise their contribution to UKUSA.

OBJECTIVE C



RELEVANT PLANS AND ACTIONS

This is a continuing commitment, actively pursued by means of liaisons between customers and GCHQ staff.

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL VII

Third Party SIGINT relationships which optimise their contribution to UKUSA.

OBJECTIVE D

[Redacted]

RELEVANT PLANS AND ACTIONS

- a.
- b.
- c.
- d.

[Redacted]

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

~~TOP SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL VIII

A survivable UKUSA SIGINT capability to ensure essential support to agreed appropriate Government authorities in any foreseeable contingency.

OBJECTIVE A

[Redacted]

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

RELEVANT PLANS AND ACTIONS

[Redacted]

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL VIII

A survivable UKUSA SIGINT capability to ensure essential support to agreed appropriate Government authorities in any foreseeable contingency.

OBJECTIVE B

[Redacted]

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

RELEVANT PLANS AND ACTIONS

- a. [Redacted]
- b. [Redacted]
- c. [Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL VIII

A survivable UKUSA SIGINT capability to ensure essential support to agreed appropriate Government authorities in any foreseeable contingency.

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

OBJECTIVE C

[Redacted]

RELEVANT PLANS AND ACTIONS

- a. [Redacted]
- b. [Redacted]
- c. [Redacted]
- d. [Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~



~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL IX

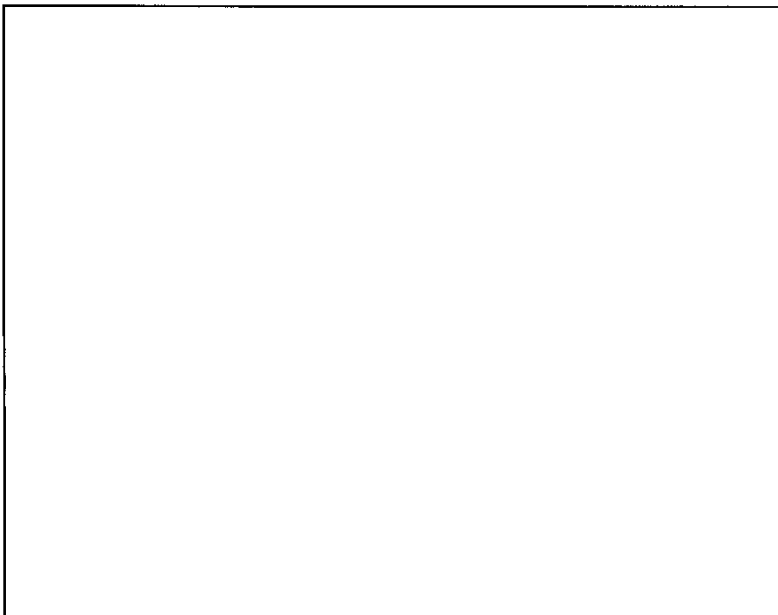
A contribution from the R&D and engineering organisations which maximizes the realisation of UKUSA goals.

OBJECTIVE A



RELEVANT PLANS AND ACTIONS

- a.
- b.
- c.
- d.
- e.
- f.
- g.
- h.
- i.
- j.



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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL IX

A contribution from the R&D and engineering organisations which maximizes the realisation of UKUSA goals.

OBJECTIVE B

[Redacted]

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

RELEVANT PLANS AND ACTIONS

- a. [Redacted]
- b. [Redacted]
- c. [Redacted]
- d. [Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL IX

A contribution from the R&D and engineering organisation which maximises the realisation of UKUSA goals.

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

OBJECTIVE C

[Redacted]

RELEVANT PLANS AND ACTIONS

- a. [Redacted]
- b. [Redacted]
- c. [Redacted]
- d. [Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~

GOAL IX

A contribution from the R&D and engineering organisation which maximises the realisation of UKUSA goals.

OBJECTIVE D

[Redacted]

RELEVANT PLANS AND ACTIONS

- a. [Redacted]
- b. [Redacted]

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

~~TOP SECRET~~  
~~HANDLE VIA COMINT CHANNELS ONLY~~



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

Serial: Q1-2193-84  
8 August 1984

[Redacted]

Head of P Staff  
Government Communications Hqs  
Cheltenham Glos., England

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

Dear [Redacted]

At our 4 May 1984 meeting at Ft. Meade, we discussed a number of topics relevant to the upcoming JMR in September, e.g., the role of the JMR as it relates to the UKUSA Planning Conference, the purpose and future substance of the JMR, etc. A subject receiving particular attention was the tracking system needed to evaluate progress made towards achieving UKUSA Joint Goals and Objectives.

We have received your paper addressing current progress made on Joint Goals and Objectives, and appreciate the synopsis of relevant plans and actions associated with each Goal. I am attaching a complementary paper that pulls together, I believe, a tracking system which has been the object of considerable discussion and review. The system is relatively straightforward, and is flexibly comprehensive to accommodate the variety of Joint Goals and Objectives it is designed to track.

We are proposing that JMR II, in the agenda item dealing with the UKUSA Planning Conference, designate the Planning Conference as the primary mechanism to assure continuing implementation of the Joint Goals and Objectives. I sense that corporate management is very supportive of a strengthened role for the Planning Conference. As such, the Conference can serve as an assured joint forum from which to maintain our purposes in the UKUSA Joint Goals and Objectives.

I would appreciate your review of the paper, and welcome your comments. I look forward to seeing you again when our continuing endeavors bring us together.

Regards,

[Redacted Signature]

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

Director of Plans

Encl:  
a/s

Doc ID: 6636914

ENCLOSURE 2

NSA FOIA Case 100386 Page 00553

Future UKUSA Planning Conferences will have as one of their specific purposes the responsibility to review and evaluate the actions taken and progress made in furtherance of UKUSA Joint Goals and Objectives. Each Conference, when addressing this topic, shall be aware of Joint Management Review (JMR) general direction and taskings relative to the Joint G&Os.

It will be the responsibility of each Planning Conference to review joint planning and evaluate continuing means of achieving the G&Os. In particular, and as the primary method of fulfilling this responsibility, the Planning Conference shall receive full and accurate accounts by joint working groups, conferences, etc., on progress made since the previous Conference regarding their specific areas of interest(s) and collaborative efforts. The Planning Conference will be responsible for measuring and evaluating these activities, and undertaking action to revise, modify, initiate, or terminate any activity, joint effort, or conference in furtherance of achieving the Joint G&Os.

ENCLOSURE

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



**UNITED  
STATES  
SIGNALS  
INTELLIGENCE  
DIRECTIVE**

**USSID FA6001**

**(U) SECOND PARTY SIGINT RELATIONSHIPS**

**ISSUE DATE: 22 August 2012**

**REVISED DATE:**

---

**(U) OFFICE OF PRIMARY CONCERN**

**(U) National Security Agency/Central Security Service (NSA/CSS)  
Foreign Affairs Directorate**

---

**(U) LETTER OF PROMULGATION, ADMINISTRATION, AND AUTHORIZATION**

**(U) Topic of  
Promulgation**

(U//~~FOUO~~) USSID FA6001 provides policy and guidance to elements of the United States SIGINT System (USSS) concerning relationships with Second Party SIGINT organizations. While USSID FA6101, "Third Party SIGINT Relationships," dated 31 October 2007, revised 29 September 2009, provides policy and guidance concerning other foreign relationships, NSA/CSS maintains a closer relationship with the SIGINT organizations in Australia, the United Kingdom, Canada and New Zealand by virtue of the British-U.S. Communications Intelligence Agreement (UKUSA), dated 5 March 1946.

**(U) USSID Edition**

(U) This USSID supersedes USSID FA6001, dated 22 March 1993, which must now be

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



destroyed.

**(U) Legal Protection of Sensitive Information** (U//~~FOUO~~) This USSID contains sensitive information that is legally protected from release to any member of the public and is to be used only for official purposes of the NSA/CSS.

**(U) Handling of USSID** (U) Users must strictly adhere to all classification and handling restrictions (see NSA/CSS Policy Manual 1-52, "NSA/CSS Classification Manual," dated 23 November 2004, revised 8 January 2007) when:

- (U) storing hard or soft copies of this USSID, or
- (U) hyperlinking to this USSID.

(U) Users are responsible for the update and management of this USSID when it is stored locally.

**(U) Location of Official USSID** (U//~~FOUO~~) The Chief, SIGINT Policy will maintain and update the current official USSID on NSANet (type "go ussid"). Selected USSIDs are also available on an access-controlled INTELINK Web page. Requests for access to the INTELINK USSID Page are granted based on mission need. (See the following INTELINK site: [https://orcon.mall.nsa.ic.gov/producer/ussid/.](https://orcon.mall.nsa.ic.gov/producer/ussid/))

**(U) Access by Contractors and Consultants** (U) **For NSA/CSS elements to include the SIGINT Extended Enterprise:**  
(U//~~FOUO~~) USSS contractors or consultants assigned to NSA/CSS Headquarters or to other elements of the SIGINT Extended Enterprise are pre-authorized for access to USSIDs via NSANet, INTELINK, or in hard-copy formats as needed to perform their jobs. However, for those sensitive USSIDs for which access is password-controlled, all users, to include contractors, must undergo additional security and mission vetting.

**(U) Outside NSA/CSS elements:**  
(U//~~FOUO~~) Non-USSS contractors or consultants working at external facilities are pre-authorized for soft-copy access to USSIDs via NSANet or INTELINK, if connectivity to those systems is allowed by the contractors' NSA/CSS sponsor. Where such connectivity is not established, any hard-copy provision of USSIDs must be authorized by the Chief, SIGINT Policy (NSA/CSS Secure Telephone System (NSTS): 966-5487, Secure Terminal Element (STE): (443) 479-1489, Defense

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

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

Switched Network (DSN): 689-5487).

(U) Access by Third Party Partners



(U) To request a shareable version:

- (U) Refer to USSID SP0002, Annex B; and
- (U) Contact the appropriate Country Desk Officer (CDO) in the NSA/CSS Foreign Affairs Directorate (DP).

(U) Executive Agent (U) The executive agent for this USSID is:

//S//  
TERESA H. SHEA  
Signals Intelligence Director

**(U) TABLE OF CONTENTS**

(U) Sections

- SECTION 1 - (U) POLICY**
- SECTION 2 - (U) RESPONSIBILITIES**
- SECTION 3 - (U) GENERAL**
- SECTION 4 - (U) TECHNICAL EXCHANGE AND VISITS**
- SECTION 5 - (U) COMBINED PARTIES AND INTEGRATED PERSONNEL ASSIGNMENTS**
- SECTION 6 - (U) SECURITY AND CLASSIFICATION**
- SECTION 7 - (U) SECOND PARTY SIGINT ORGANIZATIONS AND LIAISON OFFICES**

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

**(U) Annexes and Appendices**

**ANNEX A - (U) SIGINT LIAISON WITH AUSTRALIA, CANADA, NEW ZEALAND, AND THE UNITED KINGDOM**

**ANNEX B - (U) RELEASE OF U.S. SIGINT INFORMATION TO SECOND PARTY PARTNERS**

**SECTION 1 - (U) POLICY**

**(U) Policy**

1.1. (U//~~FOUO~~) The SIGINT Director is committed to continuing foreign partner cooperation in mutually beneficial relationships, in accordance with U.S. laws and policy, including Director of National Intelligence (DNI) and Secretary of Defense (SECDEF) guidance. The Office of the Director of National Intelligence (ODNI) establishes policy governing procedures for the overall conduct of all SIGINT arrangements with foreign governments in accordance with DCID 5/5, "Conduct of SIGINT Liaison with Foreign Governments and the Release of U.S. SIGINT to Foreign Governments."

1.2. (U//~~FOUO~~) SIGINT relationships with foreign nations, to include close international partners Australia, Britain, Canada, and New Zealand, have in the past provided, and must continue to provide a clear benefit for the United States and, as specified in DCID 6/6, "Security Controls of the Dissemination of Intelligence Information," dated 11 July 2001, promote the interests of the United States, is consistent with U.S. law, and does not pose unreasonable risk to U.S. foreign policy or national defense. U.S. SIGINT technology, resources, and collection shared with foreign partners must also enhance U.S. national interests through contributions by the SIGINT partner, support U.S. strategy when SIGINT is to be shared, and contribute to U.S. defense and intelligence goals.

**(U) Executive Agent**

1.3. (U//~~FOUO~~) The Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS) executes ODNI policy guidance in the conduct of SIGINT arrangements with Australia, Canada, New Zealand, and the United Kingdom (UK) (hereinafter referred to as Second Parties). The Second Party SIGINT organizations are the Defence Signals Directorate (DSD) for Australia, the Communications Security Establishment Canada (CSEC) for Canada, the Government Communications Security Bureau (GCSB) for New Zealand, and the Government Communications Headquarters (GCHQ) for the UK.

**SECTION 2 - (U) RESPONSIBILITIES**

(U)  
DIRNSA/CHCSS

2.1. (U//~~FOUO~~) DIRNSA/CHCSS, with the approval of the ODNI, appoints a Special United States Liaison Officer (SUSLO) for each Second Party SIGINT organization. Each SUSLO is responsible for SIGINT liaison and exchange with the applicable accredited Second Party SIGINT organization. The SUSLO represents the ODNI and DIRNSA/CHCSS in all SIGINT relationships with that Second Party, and, in so doing, executes National Intelligence Board (NIB) policy guidance.

2.2. (U//~~FOUO~~) The SUSLO facilitates direct exchange of information to ensure that NIB members obtain SIGINT information produced by the appropriate Second Party SIGINT organization. The SUSLO also assists in arranging meetings and exchanges of information between NIB members and their Second Party counterparts.

(U) NSA/CSS  
Organizations

2.3. (U//~~FOUO~~) The NSA/CSS Associate Directorate for Policy and Records (DJ) is responsible for the staff administration of the policies and procedures established in this USSID.

2.4. (U//~~FOUO~~) NSA/CSS Mission/Resource Authorities (MRAs) and Senior Functional Authorities (SFAs) are responsible for ensuring compliance with established policy concerning the release of SIGINT materials.

**SECTION 3 - (U) GENERAL**

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

(U) U.S. - Second  
Party Collaboration

3.1. (U//~~FOUO~~) U.S.-Second Party collaboration (including [redacted] [redacted] planning for emergencies, wartime operations, and combined exercises; and defining and conducting needed SIGINT research) is arranged by DIRNSA/CHCSS and the Second Party involved.

3.2. (U//~~FOUO~~) SIGINT procedures, nomenclature, and terminology are coordinated with Second Parties, using liaison channels, to ensure standardization insofar as practicable.

(U) Access to U.S.  
SIGINT

3.3. (U//~~FOUO~~) To access U.S. SIGINT information, Second Party nationals must meet and comply with all U.S. legal, security, oversight, and training guidelines. Access by a Second Party national to U.S. SIGINT organizations or U.S. SIGINT information is permitted only when the individual's clearance and Communications Intelligence (COMINT) category and subcategory access authorization have been certified, using liaison channels, and the request for access has been approved by the individual's parent organization. NSA/CSS is the final approving authority for Second Party access in accordance with Signals Intelligence Directorate (SID) Management Directive (SMD) 427, "Access to Data for Second Party Personnel Engaged in SIGINT Production," dated

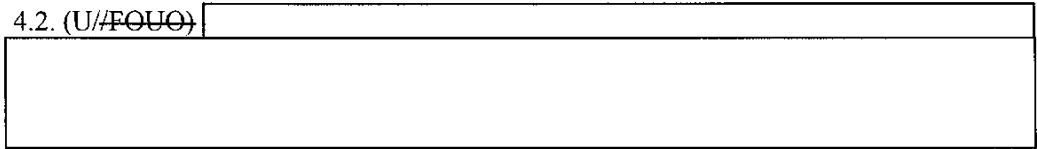
1 August 2009.

**SECTION 4 - (U) TECHNICAL EXCHANGE AND VISITS**

**(U) Technical  
SIGINT Material  
Exchange**

4.1. (U//~~FOUO~~) Technical SIGINT is exchanged between U.S. and Second Party centers or field units in accordance with the provisions of USSID AP2402, "Technical Electronic Intelligence (ELINT) Signals Analysis, and Data Forwarding Procedures," dated 23 April 2001, and the forwarding instructions in the sites' respective unit USSID.

4.2. (U//~~FOUO~~)



**(U) Visits and  
Engagements**

4.3. (U//~~FOUO~~) Proliferation and availability of secure communications technology provides numerous opportunities to convey and exchange information that were previously unavailable. While in-person visits are important, USSS personnel will be increasingly encouraged to explore other means to convey and exchange information. When a visit is necessary, approval is based on the following criteria.

a. (U//~~FOUO~~) The visit fulfills a requirement that cannot be satisfied through other established liaison channels.

b. (U//~~FOUO~~) The size of the visiting party and duration of the visit are consistent with the stated purpose of the visit and can be accommodated by the host facility.

c. (U//~~FOUO~~) The dates of the visit are convenient to the host facility.

d. (U//~~FOUO~~) The visit is mutually beneficial.

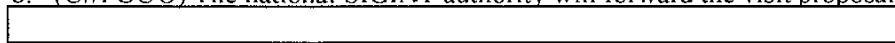
(b) (3) - P.L. 86-36

4.4. (U//~~FOUO~~) Visits between USSS elements (national to tactical) and Second Parties must be arranged in accordance with the guidelines established below. The affiliation of the visitor AND the organization to be visited determine which procedures should be followed:

4.5. (U) Second Party personnel visiting U.S. SIGINT organizations:

a. (U//~~FOUO~~) The visitor must propose the visit through the national SIGINT authority (GCHQ, CSEC, DSD or GCSB);

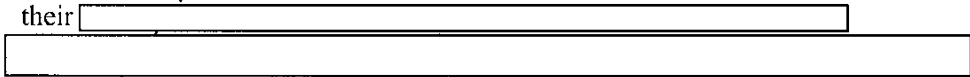
b. (U//~~FOUO~~) The national SIGINT authority will forward the visit proposal and







**EXCEPTION 1:** (U//~~FOUO~~) Intratheater visits should be processed locally (for example, SUSLOL handles proposed UK visits to U.S. SIGINT facilities in Europe; SUSLOC and SUSLOW respectively handle proposed Australian and New Zealand personnel visits to U.S. SIGINT facilities in the Pacific).

**EXCEPTION 2:** (U//~~FOUO~~) For visits to the Cryptologic Centers - The national SIGINT authority will forward the visit proposal and clearance certification to their



4.6. (U) NSA/CSS personnel visiting Second Party facilities:

a. (U) Visits to Second Party facilities within Second Party national borders:

- (U) The visitor should forward visit proposal and clearance certification message to:
  - (U//~~FOUO~~) Special United States Liaison Officer, London (SUSLOL) and SUSLOL, Cheltenham (SUSLOL CHELT) for visits to the UK;
  - (U//~~FOUO~~) Special United States Liaison Officer, Ottawa (SUSLOO) for visits to Canada;
  - (U//~~FOUO~~) Special United States Liaison Officer, Canberra (SUSLOC) for visits to Australia; and
  - (U//~~FOUO~~) Special United States Liaison Officer, Wellington (SUSLO) for visits to New Zealand.
- (U//~~FOUO~~) DP should be included on distribution for all such visit proposals, but is no longer required to show concurrence on each of these messages;
- (U//~~FOUO~~) The appropriate theater NSA/CSS Representative (NCR) should be on distribution for all such visit proposals;
- (U//~~FOUO~~)   

- (U//~~FOUO~~) The SUSLO will coordinate with Second Party Partners for these visits.

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

b. (U//~~FOUO~~) Visits to Second Party facilities based outside the Second Party national borders:

- (U//~~FOUO~~) The visitor should contact the appropriate Second Party country CDO in DP for guidance early in the trip planning process.

4.7. (U//~~FOUO~~) U.S. service cryptologic personnel visiting in-theater Second Party SIGINT facilities:

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

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

- (U//~~FOUO~~) DIRNSA/CHCSS or appropriate theater NCR must approve visits involving policy issues.

4.8. (U//~~FOUO~~) Other U.S. government personnel visiting Second Party SIGINT facilities:

a. (U//~~FOUO~~) Visits to Second Party SIGINT organizations:

- (U//~~FOUO~~) The visitor must propose the visit and forward the clearance to DP, who will coordinate within NSA/CSS and forward the proposal to the proper SUSLO; and

**EXCEPTION:** (U//~~FOUO~~) Intratheater visits should be processed locally. For example, United States European Command (USEUCOM) visits to UK SIGINT facilities should be proposed directly to SUSLOL; United States Pacific Command (USPACOM) visits to Australia or New Zealand SIGINT facilities should be proposed directly to SUSLOC and SUSLOW respectively.

- (U//~~FOUO~~) All visit proposals must be formally approved by the Second Party partner; the forwarding of clearances does not constitute visit approval. DP or SUSLO will notify visitors of approval when received from the Second Party.

b. (U//~~FOUO~~) Visits to Second Party government facilities if special intelligence certification is required:

- (U//~~FOUO~~) If the visit is to a military facility, visitor should forward a visit proposal and clearance certification message directly to the Staff Security Officer (SSO) of the Second Party military center as follows:

- (U//~~FOUO~~) For visits to UK military facilities, send a message to British

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

[Redacted]

- (U//~~FOUO~~) For visits to Canadian military facilities, send a message to

[Redacted]

- o (U//~~FOUO~~) For visits to Australian military facilities, send a message to

[Redacted]

- o (U//~~FOUO~~) For visits to New Zealand military facilities, send a message

[Redacted]

- (U//~~FOUO~~) If the visit is to a nonmilitary facility, the visitor should forward a visit proposal and clearance certification message as follows:

- o (U//~~FOUO~~) For visits to UK nonmilitary facilities, send a message to SUSLOL CHELT//SSO// with an information copy to "SUSLOL";

- o (U//~~FOUO~~) For visits to Canadian nonmilitary facilities, send a message to SUSLOO;

- o (U//~~FOUO~~) For visits to Australian nonmilitary facilities, send a message to SUSLOC; and

- o (U//~~FOUO~~) For visits to New Zealand nonmilitary facilities, send a message to SUSLOW.

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

4.9. (U//~~FOUO~~) U.S. contractors visiting Second Party SIGINT facilities for SI-level discussions:

- a. (U//~~FOUO~~) The contractor must have an NSA/CSS sponsor.

- (U//~~FOUO~~) If the contractor is working directly with a Second Party SIGINT organization and does not have an NSA/CSS sponsor, DP will fulfill the NSA/CSS sponsor role;
- (U//~~FOUO~~) The NSA/CSS sponsor is responsible for verifying clearances and forwarding the visit proposal and clearance certification message to the appropriate SUSLO; and
- (U//~~FOUO~~) Include the NSA/CSS Office of Industrial and Acquisition Security (Q13) on distribution for all contractor clearance messages.

4.10. (U//~~FOUO~~) Second Party cryptologic personnel and their contracting representatives visiting U.S. contractor facilities for SI-level discussions:

- a. (U//~~FOUO~~) [Redacted]



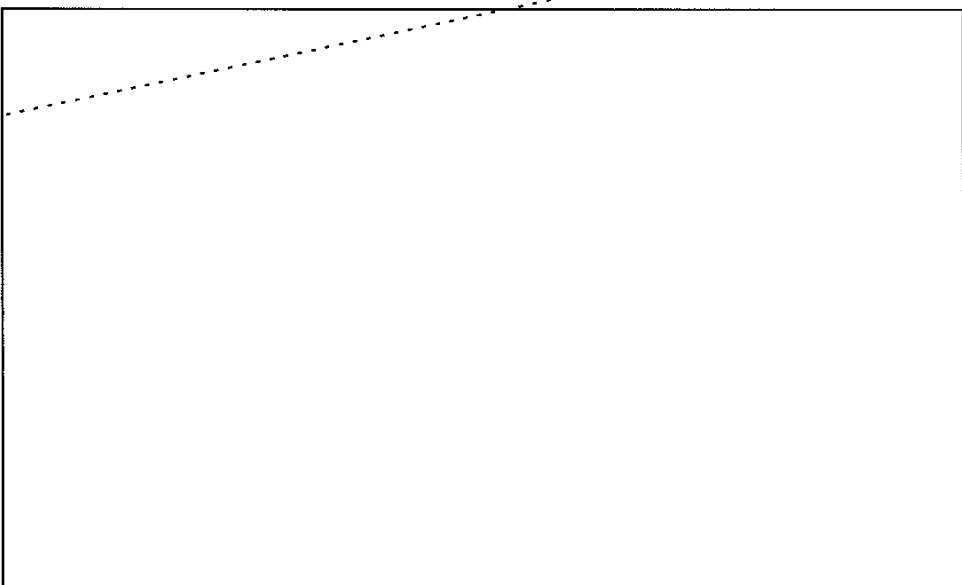
~~SECRET//SI//REL TO USA, FVEY~~

- b. (U//~~FOUO~~) DP will conduct any coordination required for the visit;
- c. (U//~~FOUO~~) The NSA/CSS sponsoring organization must complete the Clearance Certification Form (form G2901) and forward it to DP for signature; and
  - (U//~~FOUO~~) If NSA/CSS is not sponsoring the visit, the appropriate liaison office must complete form G2901 and forward it to DP for signature.
- d. (U//~~FOUO~~) DP will sign the form and forward it to the NSA/CSS Special Access Office (Q23).

(U//~~FOUO~~) Visit Proposal Messages

4.11. (U//~~FOUO~~) All visit proposal messages must be forwarded [redacted] and contain the following visitor information:

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



**SECTION 5 - (U) COMBINED PARTIES AND INTEGRATED PERSONNEL ASSIGNMENTS**

(U) SIGINT Agreements

5.1. (U//~~FOUO~~) Agreements between DIRNSA/CHCSS and Second Party SIGINT directors provide for the establishment of combined operational and research efforts and integrated personnel assignments at SIGINT locations.

(U) Second Party Integration

5.2. (U//~~FOUO~~) In accordance with NSA/CSS Policy 1-13, "Second Party Integrees," dated 29 December 2010, the integration of Second Party personnel into USSS sites will

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

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

be supported when it is beneficial to the U.S. SIGINT or mission. The establishment of these positions must be coordinated with, and approved by DP prior to staffing more fully within NSA/CSS.

**(U) Security Ramifications**

5.3. (U//FOUO) Security ramifications [redacted] associated with Second Party integreees must be considered prior to establishing and staffing any positions. In accordance with NSA/CSS Policy 1-13 and SMD 427, Second Party integreees should not be placed in positions where they might influence or represent the U.S. SIGINT decision-making process, including both contractual and policy deliberations.

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

### SECTION 6 - (U) SECURITY AND CLASSIFICATION

**(U) SIGINT Security Procedures**

6.1. (U//FOUO) SIGINT security procedures and criteria are mutually agreed to by U.S. and Second Party policy authorities and are contained in USSID SP0003.

**(U) Classification**

6.2. (U//FOUO) As of December 1983, the fact that DIRNSA/CHCSS has a relationship with any or all Second Party countries, or that they exchange liaison officers and conduct liaison concerning SIGINT, is unclassified. [redacted]

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

### SECTION 7 - (U) SECOND PARTY SIGINT ORGANIZATIONS AND LIAISON OFFICES

**(U) Second Party SIGINT Organizations**

7.1. (U//FOUO) The Second Party locations and liaison offices, and NSA/CSS liaison offices associated with Second Parties, that appear in NSA/CSS correspondence are:

~~CONFIDENTIAL//REL TO USA, FVEY~~

#### Second Party SIGINT Organizations

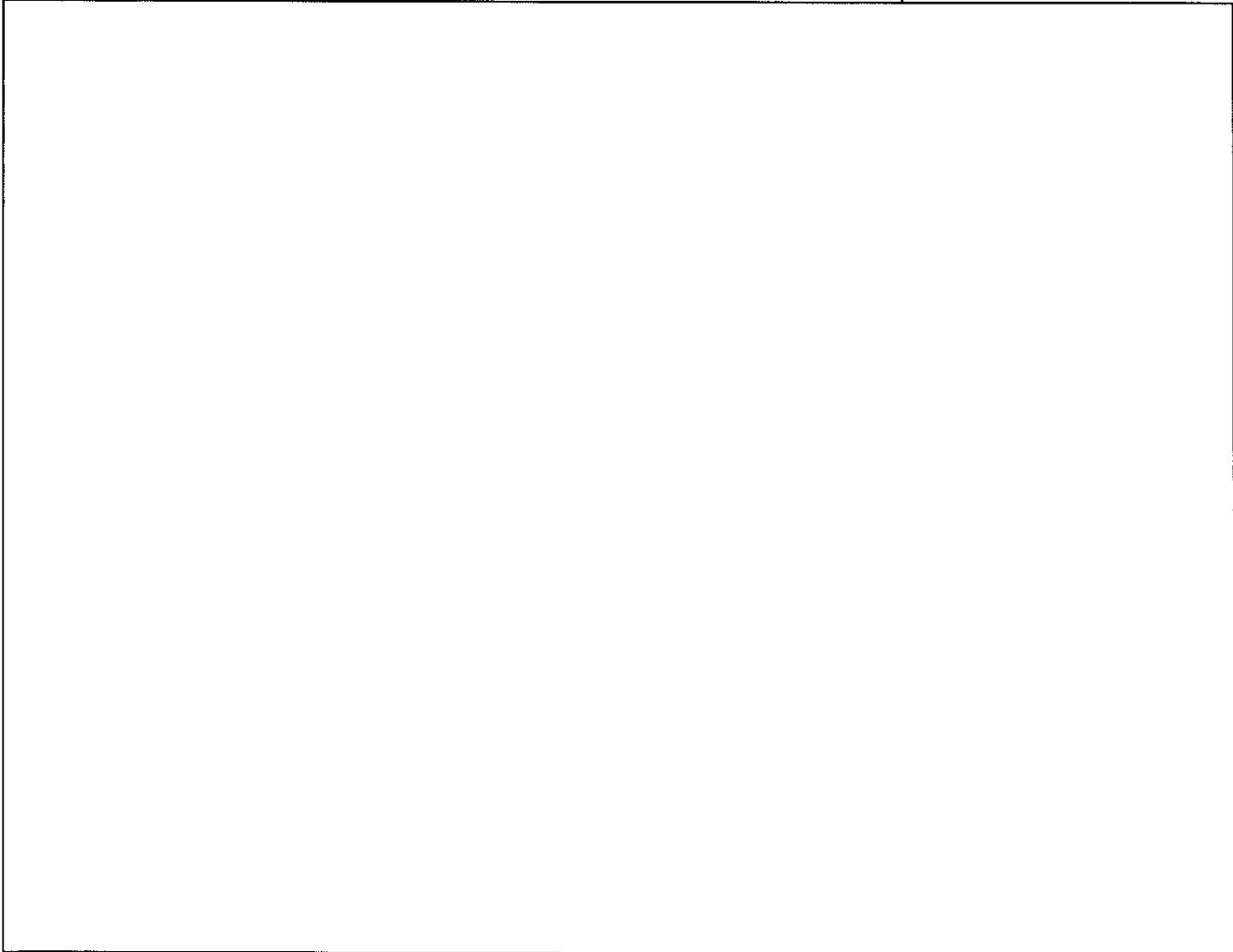
[Large redacted area]

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

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

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

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



~~CONFIDENTIAL//REL TO USA, FVEY~~

---

**USSID FA6001**  
**ANNEX A - (U) SIGINT LIAISON WITH AUSTRALIA, CANADA,**  
**NEW ZEALAND, AND THE UNITED KINGDOM**

---

**SECTION 1 - (U) PURPOSE**

**(U) Purpose**      A1.1. (U) This Annex delineates procedures and responsibilities for conducting SIGINT

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

liaison with Second Party collaborating centers.

**SECTION 2 - (U) RESPONSIBILITIES**

**(U) SUSLO** A2.1. (U) The SUSLO, as the senior representative of DIRNSA/CHCSS to the Second Party organization, is responsible for ensuring the continued effectiveness of SIGINT collaboration.

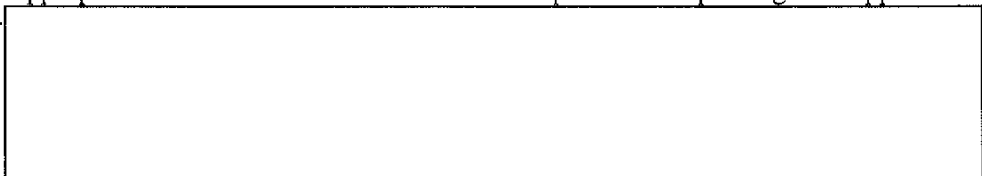
**(U) The Associate Directorate for Policy and Records** A2.2. (U//~~FOUO~~) DJ is responsible for the conduct of policy for DIRNSA/CHCSS. SID, the Information Assurance Directorate (IAD), and DP are responsible for the conduct of foreign relations planning.

**(U) Director of Foreign Affairs** A2.3. (U//~~FOUO~~) The Director, Foreign Affairs is the principal agent of DIRNSA/CHCSS for supervising the conduct of liaison with foreign partners. Within DP, DP1 (SIGINT Operations) is responsible for Second Party SIGINT relations, and DP2 is responsible for Second Party Information Assurance relations.

**(U) Commanders of the U.S. Service Cryptologic Components (SCCs)** A2.4. (U//~~FOUO~~) The commanders of U.S. SCCs, and their respective service representatives, are authorized to conduct liaison with respective in-theater Second Party military colleagues on SIGINT matters relating to the interoperability of military tactical systems, SIGINT operational capabilities, tactics, training, personnel utilization, etc. This includes exchange visits between cryptologic personnel attached to military units and other non-SIGINT organizations.

a. (~~S//SI//REL~~) Prior approval for liaison on non-routine SIGINT matters must be obtained by the SCC from DIRNSA/CHCSS. Respective SCC Headquarters and the appropriate SUSLO must be included on correspondence requesting such approval.

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



b. (U//~~FOUO~~) SCC subordinate elements must report any significant actions taken, agreements made, or subjects discussed during such liaison to DIRNSA/CHCSS, the respective SCC Headquarters, DP, and the appropriate SUSLO.

**SECTION 3 - (U) PROCEDURES**

**(U) General**

A3.1. (U//~~FOUO~~) Effective SIGINT liaison between DIRNSA/CHCSS and Second Party Partners requires the use of SUSLOs as the channels to Second Party Partners. Similarly, Second Party Partner liaison officers are channels to liaison with NSA/CSS.

A3.2. (U//~~FOUO~~) NSA/CSS Headquarters elements use "DIRNSA" (vice NSA) as the "FROM" addressee when corresponding with SUSLOs or Second Party centers.

A3.3. (U//~~FOUO~~) For administrative-related matters (Temporary Duty (TDY), personnel actions, etc.), do not include either the Second Party HQ or its liaison office at NSA/CSS as an action or information addressee.

A3.4. (U//~~FOUO~~) Information Assurance inquiries should be forwarded to the Information Assurance Directorate (IAD) with information copies to DP's SIGINT Operations Group (DP1) and Information Operations Group (DP2). Since this is a USSID (SIGINT Directive), it is NSA/CSS FAD's recommendation that the information on IA be limited to what has been proposed. IAD documentation should address foreign partner engagement.

**(U) Second Party Liaison and Collaboration**

A3.5. (U//~~FOUO~~) The SUSLOs include the SUSLOC (Canberra), the SUSLOO (Ottawa), the SUSLOW (Wellington), and the SUSLOL (London). Each SUSLO must be kept informed of developments that pertain to, or may affect, NSA/CSS and Second Party relationships.

A3.6. (U//~~FOUO~~) DSD, CSEC, GCSB and GCHQ have established

[Redacted]

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

[Redacted]

a. (U//~~FOUO~~) If it is necessary to consult these offices before approaching the SUSLO, advise the SUSLO as soon as possible thereafter. Whenever substantive information is passed orally to a liaison officer, prepare a brief Memorandum for the Record of the conversation, and forward copies to the SUSLO, DIRNSA/CHCSS, DP1, and DP2 for IA, by the most expeditious means.

b. (U//~~FOUO~~) Send to the concerned Second Party liaison office all replies to queries or actions from that office, even if the correspondence responds to a communication that has been forwarded from the director or chief of a Second Party HQ. Such correspondence must be coordinated with DP prior to release. Furnish information copies to the SUSLOs concerned.

# USSID FA6001

## ANNEX B - (U) RELEASE OF U.S. SIGINT INFORMATION TO SECOND PARTY SIGINT ORGANIZATIONS

### SECTION 1 - (U) PURPOSE

**(U) Purpose** B1.1. (U//~~FOUO~~) This Annex sets forth the procedures for releasing U.S. SIGINT information to the Second Party SIGINT organizations.

### SECTION 2 - (U) GENERAL

**(U) Second Party Collaboration** B2.1. (U//~~FOUO~~) NSA/CSS and the Second Party Partners collaborate on a wide range of targets. The specific targets and degree of collaboration may change from time to time by mutual agreement and should be documented by a Memorandum of Understanding/Memorandum of Agreement (MOU/MOA) or a Division of Effort (DOE) statement. Copies of all MOU/MOAs must be provided to the NSA/CSS Office of Corporate Policy (DJ), DP and SID SIGINT Policy. If a DOE Statement between NSA/CSS and Second Party elements is used to document efforts against similar targets, a copy of this statement must be provided to DP1.

**(U) SIGINT Material** B2.2. (S//SI//REL) Second Party Partners receive raw traffic, technical material, and serialized SIGINT reports derived from the U.S. effort on mutual targets, in accordance with U.S. government policy and guidelines to include SMD 427, as applicable.

**(U) Intelligence Information Requirements** B2.3. (S//SI//REL) Second Party Partners require intelligence information on issues impacting international relations, and on events related to the partners' political, economic, military, or security interests. However, no U.S. SIGINT information will be used or disseminated by Second Party Partners in a way that contradicts U.S. government policy and national security goals and objectives or is inconsistent with U.S. law. In addition to serialized reports furnished to Second Party Partners to meet the specific intelligence requirements, consideration must also be given to:

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

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

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

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

[Redacted]

c. ~~(S//SI//REL)~~  
[Redacted]

### SECTION 3 - (U) RESPONSIBILITIES

**(U) NSA/CSS Senior Management** B3.1. ~~(U//FOUO)~~ NSA/CSS Deputy Directors/Associate Directors/Chiefs are responsible for ensuring compliance with established procedures when releasing SIGINT material under their purview to Second Party Partners. They are also responsible for providing any attendant technical support.

**(U) Information Sharing Services** B3.2. ~~(U//FOUO)~~ NSA/CSS SID Information Sharing Services (S12) maintains records of serialized reports, including field-produced serialized reports, that are released to Second Party Partners. Proposed distribution changes must be coordinated with S12 and DP1. S12 will review SIGINT exchanges with Second Party Partners that also involve distribution to a third nation, such as in combined exercises.

### SECTION 4 - (U) PROCEDURES

**(U) Release of SIGINT Material** B4.1. ~~(U//FOUO)~~ SIGINT material relevant to the requirements of a Second Party Partner is directly forwarded to the partner location.

B4.2. ~~(U//FOUO)~~ Release of new categories or types of SIGINT material is to be coordinated with DP1 and S12.

B4.3. ~~(U//FOUO)~~ If U.S. SIGINT materials are required by a particular Second Party Partner, but cannot be released because of restrictions imposed by the producing, procuring, or supplying agency, S12 will review the need and coordinate with DP1.

**Proceed To:**

[NSA](#) | [Director](#) | [SID](#) | [SID Staff](#) | [SID Policy](#) | [USSID Index](#)

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



# SIGNALS INTELLIGENCE DIRECTORATE

## MANAGEMENT DIRECTIVE 427

Issue Date: 01 August 2009  
Revised Date: 28 December 2013  
Second Rev: 14 September 2015

POC: S02

---

### (U) ACCESS TO CLASSIFIED U.S. INTELLIGENCE INFORMATION FOR SECOND PARTY PERSONNEL

---

**(U) Purpose** (U//~~FOUO~~) This document provides guidance for granting Second Party SIGINT personnel access to classified U.S. intelligence information in accordance with Department of Defense Directive (DoDD) C-5230.23, "Intelligence Disclosure Policy" (Ref A); Director of Central Intelligence Directive 6/7, "Intelligence Disclosure Policy" (Ref B); and DoDD 5240.1-R, "Procedures of DoD Intelligence Components that Affect U.S. Persons" (Ref C)

*NOTE: (U) Underlined terms are defined under Annex D Definitions.*

**(U) Scope** (U) This Signals Intelligence Directorate (SID) Management Directive applies to all U.S. SIGINT production elements located at NSA Headquarters (NSAW) and across the United States SIGINT System (USSS).

(U) This guidance supersedes all previously approved SIGINT Directorate guidance and authorizations for Second Party access to classified U.S. intelligence information. Second Party personnel who require access for the performance of the SIGINT mission must be re-justified and resubmitted for approval by the SIGINT Director or Deputy Director.

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



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

(U) All new requests for Second Party accesses after the date of issue of this document must follow the guidelines herein.

---

//s//

RONALD S. MOULTRIE  
Signals Intelligence Director

DISTRIBUTION:

Signals Intelligence Directorate, All  
SIGINT Enterprise, Field, All  
Office of General Counsel  
Office of Corporate Policy

---

**(U) BACKGROUND**

---

- (U) Background**
1. (U) NSA/CSS has a tradition of signals intelligence (SIGINT) collaboration with its Second Party SIGINT Partners that has served us well. NSA/CSS and the Intelligence Community (IC) have benefited from this exchange and have broadened and improved U.S. knowledge and capabilities. Notwithstanding our special partnerships with our Second Party SIGINT Partners, NSA/CSS must first ensure that activities with our partners comply with all U.S. legal and policy guidelines. This management directive is established to define, document, and implement internal procedures to ensure consistency and compliance with all legal and policy guidelines.
  2. (U) Granting access to Second Party personnel to classified U.S. intelligence information must be done in accordance with procedures established within NSA/CSS and consistent with policies and procedures of the Director of National Intelligence and the Secretary of Defense. In addition, NSA/CSS, first and foremost, has a responsibility to protect intelligence information that contains or may contain equities of other members of the IC. Granting access to or approving release of information to Second Party personnel applies equally to SIGINT as well as to intelligence gathered under the authority of other IC agencies, or any intelligence from those agencies that is fused with SIGINT (to include that from collaborative access efforts). Often, only the originating agency or element may be aware of the sensitivities of the intelligence information, therefore that agency's permission must be obtained prior to sharing.

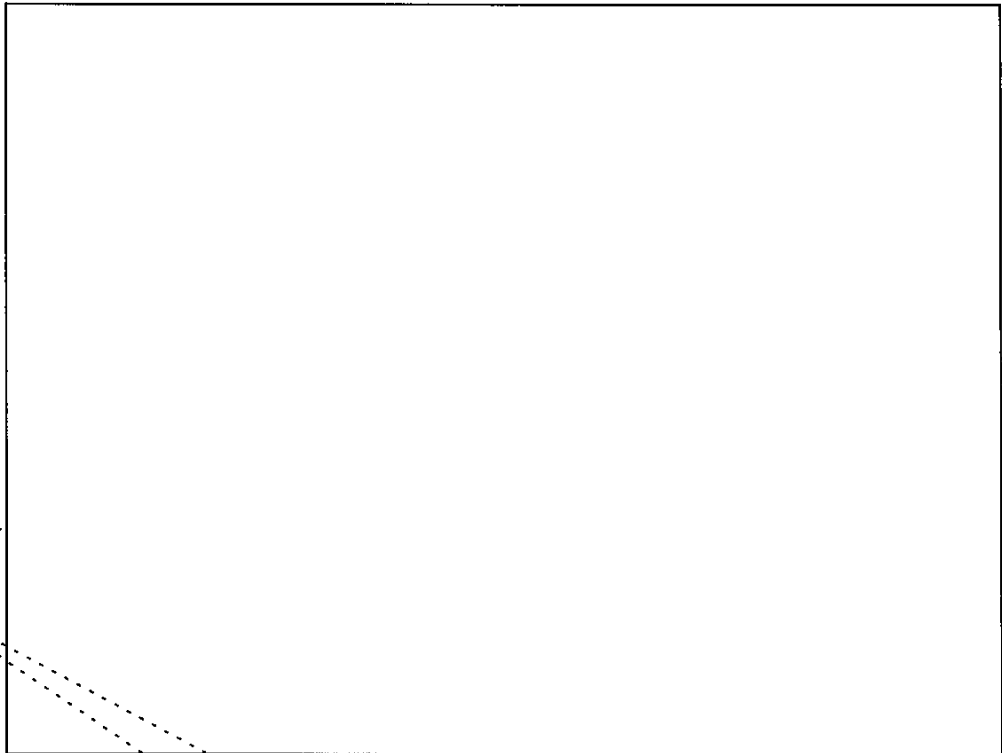
~~CONFIDENTIAL//SI//REL TO USA, FVEY~~

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

3. (U//FOUO) Per Director of Central Intelligence Directive (DCID) 5/5P, "Conduct of Liaison with Foreign Governments and Release of U.S. SIGINT to Foreign Governments" (Ref D), DIRNSA/CHCSS is the executive agent of the U.S. Government for the conduct of SIGINT arrangements with the Second Parties. DCID 6/6, "Security Controls on the Dissemination of Intelligence Information" (Ref E), specifies that intelligence may be shared with foreigners (including Second Party personnel) to the extent such sharing promotes the interests of the United States, is consistent with U.S. law, does not pose unreasonable risk to U.S. foreign policy or national defense, and is limited to a specific purpose and normally of limited duration. The directive mandates NSA/CSS' responsibility to apply appropriate controls to and accountability for the access to or release of intelligence to our foreign partners.

**(U) Data Categories**

4. (U//FOUO) For the purposes of this policy, data, databases, and data sets maintained by NSA/CSS will be categorized as follows:



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

**(U) POLICY**

**(U) Approval Authorities**

5. (U//FOUO) [Redacted]

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

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

[Redacted]

6. (U//FOUO) [Redacted]

[Redacted]

7. (U//FOUO) If the Second Party person is an integree as defined in NSA/CSS Policy 1-13, "Second Party Integrees" (Ref F), then [Redacted] will be recorded by the integree's supervisor and the appropriate Foreign Affairs Directorate desk officer shall be notified.

8. (U//FOUO) Second Party personnel access to NSA/CSS-maintained databases or data sets that only contain classified information marked releasable to that partner, or databases that are capable of restricting access only to that data which is marked releasable to that partner, regardless of the originating agency of the data, will be granted to Second Party personnel in accordance with Annex A to this policy. Approval authority for Second Party access marked releasable resides with the relevant SIGINT Directorate Deputy Director or Associate Director (i.e., DDEM/ADDEM, DDAP/ADDAP, DDDA/ADDDA, and ADD/SSG), NTOC DIR, and SUSLOs Canberra, London, Ottawa, and Wellington).

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

9. (U//FOUO) [Redacted]

[Redacted]

(U//FOUO) [Redacted]

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

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

[Redacted]

NOTE: (U//FOUO)

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

[Redacted]

10. (U//FOUO)

[Redacted]

11. (U//FOUO) The NSA/CSS Director, the NSA/CSS Deputy Director, or authorized Designated Intelligence Disclosure Officers (DIDOs) may authorize release to a Second Party Integree of classified U.S. intelligence that bears no specific control markings (i.e., that is not marked with "NOFORN," "REL TO," or another control marking such as "ORCON"). The details of the DIDO program and authorities may be found in DCID 6/7, "Intelligence Disclosure Policy." and the list of designated NSA/CSS DIDOs.

**(U) Data Uses**

12. (U//FOUO) Access to data by or release of data to Second Party personnel does not convey authorization or approval for Second Party follow-on use. Further use guidance will accompany each Second Party access provision.

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

[Redacted]

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

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

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



**(U) Termination of Access** 15. (U//~~FOUO~~) When a Second Party person changes work assignments or locations, any access to NSA/CSS maintained data, databases, or data sets granted through an NSA/CSS approval process (such as the SIGINT Contact Center (SCC)) is similarly terminated in accordance with SID Management Directive 421, "United States SIGINT System Database Access" (Ref H).

**(U) Emergencies** 16. (U) For emergency sharing authorization, the NSA Director or Deputy Director and/or the SIGINT Director and Deputy Director are the sole approving authorities. Emergency situations are defined and will be implemented per guidance in DCID 6/6, Section 10.

---

**(U) ANNEX A  
ACCESS TO RELEASABLE DATA**

---

**(U) General** A.1. (U//~~FOUO~~) Second Party personnel, whether integrated into an NSA/CSS established SIGINT production element or assigned to a Second Party SIGINT organization, may be granted access to NSA/CSS maintained SIGINT databases and data sets that contain only data marked as releasable to that Second Party partner or databases that are capable of restricting access only to that data which is marked as releasable to that partner. All Second Party personnel accessing NSA/CSS maintained databases and data sets must adhere to the same standards as U.S. SIGINT personnel with regard to U.S. intelligence oversight, to include U.S. Intelligence Oversight Officers (IOOs), U.S. auditors, and appropriate intelligence oversight training and reporting programs. Second Party Integrees shall not be assigned positions for which access to NOFORN information is routinely required, without prior approval from all originators of that information.

**(U) Access for Personnel in Second Party SIGINT** A.2. (U//~~FOUO~~) Second Party SIGINT elements requiring access to releasable databases or data sets must first be registered in the NSA/CSS Mission Correlation Table (MCT) in accordance with SID Management Directive 422, "USSS Mission Delegation" (Ref I), by following the SID SIGINT Contact

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

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

**Elements**

Center (SCC) process

[redacted] for Sponsors and Data Masks. Given that these will be Second Party missions, the relevant Analysis and Production Global Capability Managers will coordinate on, but not approve, the registration of the mission and the associated databases.

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

A.3. (U//FOUO) Second Party SIGINT elements will work with the appropriate Senior U.S. Liaison Office (SUSLO) and the appropriate NSA/CSS Foreign Affairs Directorate (FAD) Desk Officer to draft and coordinate the access request for registration in the MCT. The FAD Desk Officer will function as the Sponsor into the SCC process. The Desk Officers will work with SID Oversight and Compliance (O&C) Compliance and Verification Team [redacted] [redacted] to determine the appropriate oversight path, training, and auditing requirements for each element and associated database being registered in the MCT. If access is approved, access to individual releasable databases is then granted through the SCC standard procedure.

**(U) Access for Second Party Integrees**

A.4. (U//FOUO) Second Party SIGINT personnel integrated into NSA/CSS SIGINT production elements under NSA/CSS Policy 1-13, "Second Party Integrees" will be sponsored for access through established procedures in SIGINT Management Directive 421. Supervisors of Second Party integrees must maintain a list of any databases or data sets accessed by the integree and will notify the appropriate FAD Desk Officer of any changes during the integree's assignment which would require a change to access. Approval authority for database and/or data set access to "NSA/CSS or IC Not-Releasable" will be the NSA Director, Deputy Director, SIGINT Director or SIGINT Deputy Director.

**(U) Termination of Access**

A.5. (U//FOUO) When Second Party personnel change work assignments or locations, any access to SIGINT databases or data sets will be terminated immediately. The SIGINT production element's NSA/CSS Sponsor or Intelligence Oversight Officer (IOO) is responsible for requesting the database System Administrators to terminate and remove the individual's accounts from their systems in accordance with SID Management Directive 421. For Second Party Integrees, the immediate supervisor (U.S. or Second Party) is responsible for the termination of accesses and will notify the appropriate FAD desk officer and personnel in accordance with SID Management Directive 421.

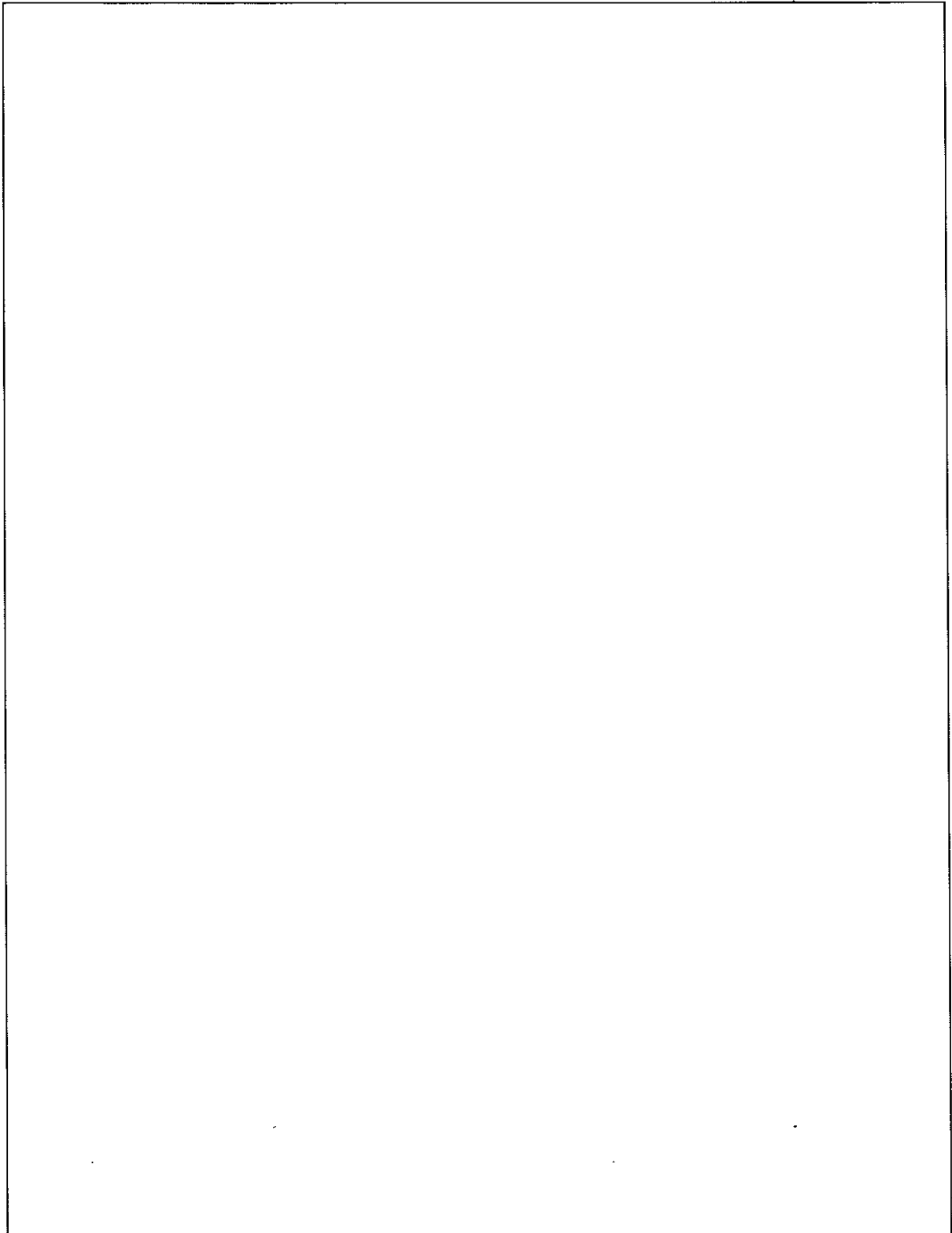
(b) (3) - P.L. 86-36

**(U) ANNEX B**

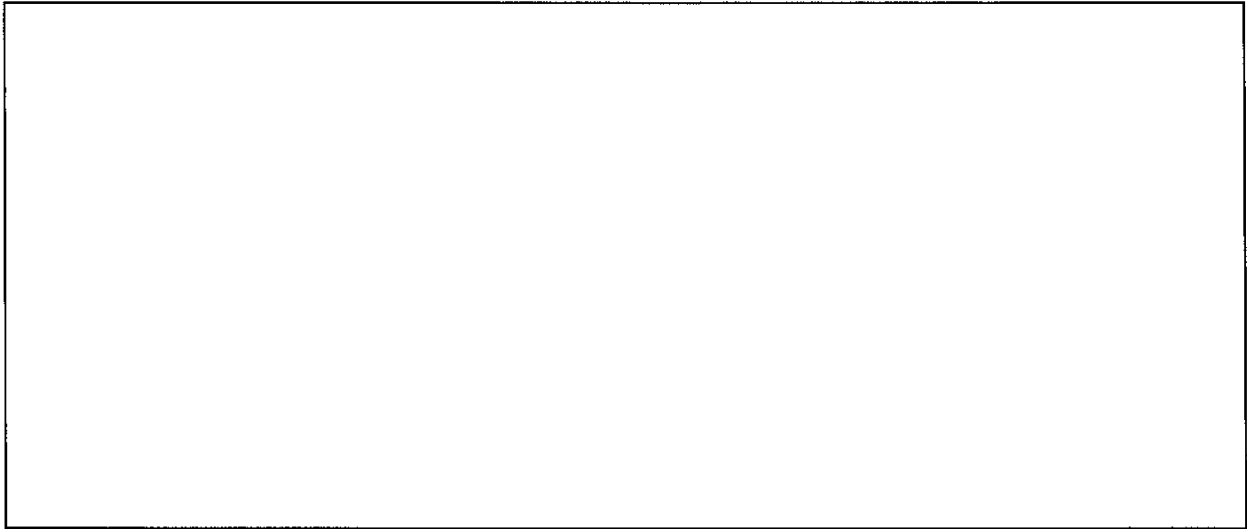


~~CONFIDENTIAL//SI//REL TO USA, FVEY~~

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



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



---

**(U) ANNEX C  
REFERENCES**

---

- a. (U//~~FOUO~~) Department of Defense Directive (DoDD) C-5230.23, "Intelligence Disclosure Policy"
- b. (U//~~FOUO~~) Director of Central Intelligence Directive 6/7, "Intelligence Disclosure Policy"
- c. (U//~~FOUO~~) DoDD 5240.1-R, "Procedures of DoD Intelligence Components that Affect U.S. Persons"
- d. (U//~~FOUO~~) Director of Central Intelligence Directive (DCID) 5/5P, "Conduct of Liaison with Foreign Governments and Release of U.S. SIGINT to Foreign Governments"
- e. (U//~~FOUO~~) Director of Central Intelligence Directive (DCID) 6/6, "Security Controls on the Dissemination of Intelligence Information"
- f. (U//~~FOUO~~) NSA/CSS Policy 1-13, "Second Party Integrees"
- g. (U//~~FOUO~~) NSA/CSS POLICY 1-41, "The NSA/CSS Exceptionally Controlled Information (ECI) System"
- h. (U//~~FOUO~~) SID Management Directive 421, "United States SIGINT System Database Access"
- i. (U//~~FOUO~~) SID Management Directive 422, "USSS Mission Delegation"



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

- j. (U//FOUO) Executive Order (E.O.) 12333, "United States Intelligence Activities"
- k. (U//FOUO) National Security Act of 1947
- l. (U//FOUO) UKUSA Agreement, dated 5 March 1946

**(U) ANNEX D  
DEFINITIONS**

**(U) Data Set** D.1. (U) For the purpose of this policy, a large collection of intelligence data that has not been evaluated for foreign intelligence or minimized to protect U.S. identities but is not a formal database subject to the SIGINT Contact Center (SCC) process or a similar access control. A data set may also be a data feed such as would be needed for a research/development effort.

**(U) Database** D.2. (U//FOUO) For the purpose of this policy, a structured collection of records or data that is stored in a computer system and organized in a data management system for quick retrieval of those records. A database is generally subject to the SCC process or a similar access control and listed

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

[Redacted]

**(U) Designated Intelligence Disclosure Official (DIDO)** D.3. (U) The heads of departments and agencies with organizations in the Intelligence Community or the heads of such organizations, and their specifically designated subordinates whose names and positions are certified to the Director National Intelligence (DNI) in writing, and other U.S. officials designated by the DNI.

**(U) Exceptionally Controlled Information (ECI)** D.4. (U) COMINT sub-control system/sub-compartment to protect TOP SECRET exceptionally sensitive COMINT sources, methods and activities.

**(U) Evaluated, Minimized Traffic (EMT)** D.5. (U) Traffic that has been minimized for U.S. identities and assessed for foreign intelligence value.

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

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

**(U) Integree**

D.6. (U//~~FOUO~~) The term “integree” in this document refers to Second Party Partner personnel integrated into or detailed to SIGINT production element (as defined in USSID CR1610) who, when integrated into an NSA/CSS environment, are working solely under the direction and operational control of the DIRNSA/CHCSS to conduct SIGINT activities that support information needs validated by NSA/CSS in accordance with NSA/CSS authorities, rules, and regulations. Integrees may be civilians or military members. Integrees must be approved in accordance with NSA/CSS Policy 1-13, “Second Party Integrees.”

**(U) Intelligence**

D.7. (U) Includes the following information, whether written or in any other medium, classified pursuant to Executive Order 12958 or any predecessor or successor Executive Order:

- a. (U) Foreign intelligence and counterintelligence defined in the National Security Act of 1947 (Ref K), as amended and Executive Order 12333;
- b. (U//~~FOUO~~) Information describing U.S. foreign intelligence and counterintelligence activities, sources, methods, equipment, or methodology used for the acquisition, processing, or exploitation of such intelligence; foreign military hardware obtained through intelligence activities for exploitation and the results of the exploitation; and any other data resulting from U.S. intelligence collection efforts; and

(U) Information on Intelligence Community protective security programs (e.g. personnel, physical, technical, and information security).

**(U) Intelligence Community (IC)**

D.8. (U) The Intelligence Community comprises the:

- Central Intelligence Agency (CIA),
- National Security Agency (NSA),
- Defense Intelligence Agency (DIA),
- Bureau of Intelligence and Research (within the Department of State),
- National Geospatial-Intelligence Agency (NGA),
- National Reconnaissance Office (NRO),
- Intelligence and Counterintelligence Elements of the Army, Navy, Air Force, Marine Corps, and Coast Guard.
- Staff elements of the Director of National Intelligence (DNI), and
- Intelligence elements of the:

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

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

- o Drug Enforcement Administration,
- o Federal Bureau of Investigation (FBI),
- o Department of Justice,
- o Department of the Treasury,
- o Department of Homeland Security, and
- o Department of Energy.

**(U) SIGINT Content**

D.9. (U) The actual information (e.g., voice, data, or video) exchanged between one or more individuals, systems or devices.

**(U) SIGINT Metadata**

D.10. (U//~~FOUO~~) Refers to structured "data about data." Metadata includes all information associated with, but not including content, and includes any data used by a network, service, or application to facilitate routing or handling of a communication or to render content in the intended format. Metadata includes, but is not limited to, dialing, routing, addressing, or signaling information and data in support of various network management activities (e.g. billing, authentication or tracking of communicants).

**(U) Mission Correlation Table (MCT)**

D.11. (U//~~FOUO~~)

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

**(U) Product**

D.12. (U) Foreign intelligence (derived from SIGINT processes) that is made available in readable form to authorized recipients in response to stated or implied Information Needs. SIGINT Product reporting standards are governed United States Signals Intelligence Directives (USSIDs) and other SIGINT policy.

**(U) Raw SIGINT Data**

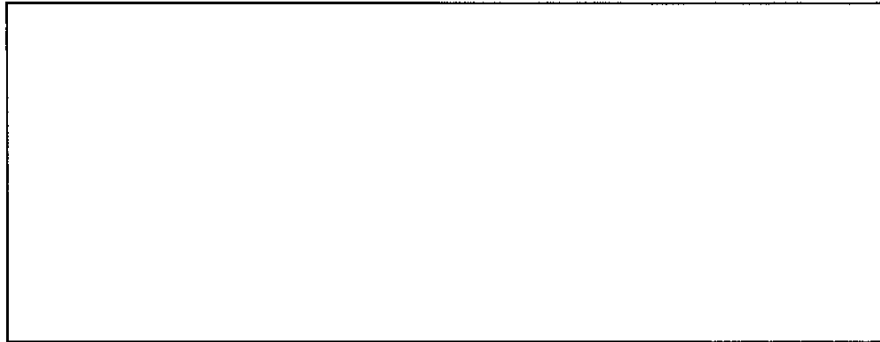
D.13. (~~C//SI//REL TO USA, FVEY~~) Raw SIGINT data is any SIGINT data acquired either as a result of search and development or targeted collection operations against a particular foreign intelligence target **before** the information has been evaluated for foreign intelligence AND minimization purposes. It includes, but is not limited to, unevaluated and/or unminimized

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

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

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

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



**(U) Second Party** D.14. (U) Any of the four countries with which the U.S. Government maintains close, cooperative SIGINT and Information Assurance (IA) relationships: Australia, Canada, New Zealand, and the United Kingdom (UK). The strategic alliance among these nations stems from the strong cryptologic partnerships that developed during World War II and were first formalized in the UKUSA Agreement (Ref L), dated 5 March 1946.

**(U) Second Party SIGINT Partners** D.15. (U) The following SIGINT organizations, their subordinate units, and other cryptologic units affiliated with, or approved by, the National SIGINT authority. The organizations are:  
a. (U) UK - Government Communications Headquarters (GCHQ)  
b. (U) Canada - Communications Security Establishment Canada(CSEC)  
c. (U) Australia - Defence Signals Directorate (DSD)  
d. (U) New Zealand - Government Communications Security Bureau (GCSB)

**(U) Second Party SIGINT Personnel** D.16. (U) This includes all Second Party personnel assigned to and working under the SIGINT Authorities of the respective Second Party Partner organization. This includes Second Party civilian, military, and contractor personnel.

**(U) SIGINT Production Element** D.17. (U) A formally recognized and documented element (organization, unit) that executes at least one of the SIGINT production functions (collection, processing, analysis, retention, and dissemination) performed by United States SIGINT System (USSS) and/or foreign SIGINT production personnel (collectors, cryptanalysts, intelligence analysts, linguist, reporters, SIGINT development analysts, research personnel, staff, support elements, and managers) necessary for the conduct of an assigned SIGINT mission.

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

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

**(U) Stakeholder**

---

D.18. (U) Stakeholders in the access of data Not Releasable by a Second Party person would be any office with an equity in the information. This list might include:

- S1 Customer Relations,
- S2 Analysis and Production,
- S3 Data Acquisition,
- SSG SIGINT Development,
- Associate Deputy Directorates for Counter Terrorism (ADD/CT) and Technical SIGINT and Electronic Warfare(ADD/TSE),
- National Threat Operations Center (NTOC),
- NSA/CSS Commercial Solutions Center (NCSC),
- Research Directorate (RAD),
- Associate Directorate for Education and Training (ADET),
- Associate Directorate for Security and Counterintelligence (ADS&CI), and
- National Cryptologic Representatives and Senior Liaison Officers, as appropriate.

**(U) United States SIGINT System (USSS)**

---

D.19. (U) The United States SIGINT System (USSS) is the SIGINT part of the United States Cryptologic System (USCS) and refers to the U.S. Government SIGINT activities worldwide under the direction of the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS). The USSS is composed of the NSA/CSS SIGINT Directorate, the SIGINT functions and elements of the military departments, and other governmental elements (other than the Federal Bureau of Investigation) authorized to perform SIGINT activities under the direction and authority of the DIRNSA/CHCSS.

---

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

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~



NATIONAL SECURITY AGENCY  
CENTRAL SECURITY SERVICE  
NSA/CSS POLICY 6-20



Issue Date: 31 March 2014  
Revised: 8 November 2016

---

(U) SECOND PARTY ACCESS TO NSA/CSS TS/SCI CLASSIFIED INFORMATION SYSTEMS

(U) PURPOSE AND SCOPE

(U) This policy defines processes and procedures for Second Party access to NSA/CSS classified information systems (ISs). This policy applies to all United States Cryptologic System (USCS) organizations that sponsor Second Party integrees, USCS personnel who initiate or approve requests for Second Party personnel access to U.S. classified intelligence and cryptographic information, and USCS personnel who implement Second Party personnel and systems access to any NSA/CSS classified ISs.

RICHARD H. LEDGETT, JR.  
Acting Director, NSA

Endorsed by  
Associate Director for Policy

(U) Encl:  
Annex – Second Party Access Information

(U) DISTRIBUTION:  
TS23  
DJ1  
DJ2 (Vital Records)  
DJ6 (Archives)

(U) This Policy 6-20 supersedes NSA/CSS Policy 6-20 dated 2 July 2007.  
(U) OPI: NSA/CSS IT Policy, TS23, 303-1896s.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

(U) This Policy 6-20 supersedes NSA/CSS Policy 6-20 dated 2 July 2007. The Chief, Policy approved an administrative update on 26 February 2015 to reflect new guidance on limited administrator access, align the definition of Second Party Integree with NSA/CSS Policy 1-13, and make other administrative changes. The Chief, Policy approved an administrative update on 2 November 2015 to update the definition "Authorizing Official." The Chief, Strategy, Plans, and Policy approved an administrative update on 8 November 2016 to enable qualified Second Party Liaison officers to routinely obtain direct access to NSANet. The administrative update also clarifies the terms 'second party personnel' and 'second party integrees', and makes their use more consistent; improves accuracy in specifying NSANet access type; clarifies a Second Party and Multinational Affairs Division (P523) responsibility; updates definitions; and makes minor administrative updates.

(U) OPI: Technology Policy, P12T, 717-0220s.

(U) No section of this document shall be released without approval from the Office of Policy (P12).

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

(U) POLICY

1. (U) It is the policy of NSA/CSS to share with Second Party *Cryptologic* partners all information relevant to the arrangements outlined in "U.K.-U.S. Communications Intelligence Agreement (UKUSA)" (Reference a) and subsequent bilateral understandings with each Second Party partner as outlined in [redacted] (Reference b), NSA/GCHQ/DSD/CSE/GCSB "Second Party Intranet Connection MOU" (Reference c), and [redacted] (Reference d).

2. (U) Second Party system access shall be provided in accordance with the requirements specified in Intelligence Community Directive 503, "Intelligence Community Information Technology Systems Security Risk Management" (Reference e).

3. (U//~~FOUO~~) Second Party Personnel may not perform information technology (IT) systems administrative functions or be granted *privileged access* on NSA/CSS IT systems, with the exception of limited administrative privileges in direct support of mission requirements (i.e., a virtual machine or workstation the administrative access to which is expressly required for mission purposes).

4. (U) Second Party system connection and access policy agreements between the USCS *information steward* and each Second Party country shall be established in a Memorandum of Understanding (MOU). Documents will be maintained and posted by Office of Policy (P12) on *NSA/CSS Classified Network (NSANet)*.

5. (U) Second Party integrees and Second Party Liaison officers who meet the access requirements in this policy shall routinely be given direct access to NSA/CSS ISs via individual NSA/CSS accounts.

6. (U) *Second Party Headquarters Personnel* shall routinely access NSA/CSS classified ISs indirectly via the Second Party proxy server.

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Policy 6-20

Dated: 31 March 2014

7. (U/~~FOUO~~) Second Party Personnel who are not eligible for direct access and whose requirements cannot be accommodated via the proxy server may request an *exception* to obtain direct access to NSA/CSS IS via an individual NSA/CSS account.

8. (U) All requests for Second Party direct access to NSA/CSS ISs shall be approved by the Second Party authority with parallel responsibility to NSA/CSS mission or mission-support information (e.g., signals intelligence (SIGINT), information assurance (IA), research) before presentation to NSA/CSS for consideration. Second Party requests for individual NSANet accounts must be authorized in writing by the responsible Second Party authority.

9. (U) All Second Party personnel who require direct access to classified NSA/CSS ISs for the performance of a SIGINT production mission must also follow the guidance within:

- a. (U) SIGINT Directorate (SID) Management Directive 421, "United States SIGINT System Database Access" (Reference f);
- b. (U) SID Management Directive 422, "USSS Mission Delegation" (Reference g);  
and
- c. (U) SID Management Directive 427, "Access to Classified U.S. Intelligence Information for Second Party Personnel" (Reference h).

10. (U) For direct access to NSA/CSS classified ISs, eligible Second Party personnel must be appropriately cleared and approved by the Second Party and Multinational Affairs Division (P523). In addition, Second Party integrees must be sponsored by a *Global Enterprise Leader*.

11. (U) All Second Party personnel who have obtained an NSANet user account shall complete NSA/CSS Information Assurance training (e.g., OIAC1180, "Cyber Awareness Challenge," OVSC1000, "Intelligence Oversight Training") prior to access and yearly thereafter.

12. (U) All Second Party personnel with direct access to NSANet must obtain and use Cryptologic Agencies Domain certificates if possessing citizenship in a Five Eyes country. Additional information can be found on the NSA Corporate Public Key Infrastructure (PKI) Information Page;

13. (U) All Second Party personnel with direct access to NSA/CSS ISs shall be subject to all NSA/CSS Information Technology policies and procedures.

14. (U) The citizenship of all Second Party personnel given individual NSANet accounts shall be uniquely identified in the NSA/CSS Directory Service (i.e., SEARCHLIGHT) in order to provide strong network and ISs access control.

15. (U) Second Party personnel with individual NSANet accounts may be directly connected only to those NSA/CSS classified ISs required to perform sponsored functions. For integrees, the sponsoring organization shall be the authority to identify what is required and shall

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~



have a process to account for the systems and information accessed by the integratee. ~~The System Security Plans (SSPs)~~ of all systems identified for Second Party integratee access must be updated to reflect this access.

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

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

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

19. (U) All Second Party access to non-NSA/CSS information on NSA/CSS ISs shall be controlled in accordance with an agreement with the information steward or procedures established by the information steward. Access to ISs containing non-NSA/CSS information must be approved, in writing, by the originating agency of the data, and documented in the SSP.

20. (U) Under no circumstances will any Second Party Personnel to include partners, liaison officers or integratees be provided direct access to NSA/CSS ISs that are used to generate, produce, or electronically track and distribute U.S.-only keying materials, or Nuclear Command and Control Information Assurance Materials (NCCIM).

21. (U) All Second Party personnel who no longer require access to NSA/CSS classified ISs shall have their access terminated upon completion of those specific official duties. This access is not transferable. If Second Party personnel require access in a new position, they must reapply for the access based on their new duties.

**(U) PROCEDURES**

**22. (U) Procedures for Second Party Indirect Access to NSA/CSS Information Systems via Second Party Proxy Server:**

a. (U) Written authorization is not required for Second Party personnel access to NSA/CSS ISs via Second Party proxy servers; and

b. (U) Second Party personnel are not required to register with NSA/CSS before accessing NSA/CSS resources via Second Party proxy servers.

23. (U) **Procedures for Second Party Direct Access to NSA/CSS Information Systems:** As noted above, Second Party liaison officers and integrees at NSA/CSS will be routinely sponsored for accounts on NSANet. Other Second Party personnel may be approved for such access on a case-by-case basis. The following procedures, therefore, apply to all Second Party liaison officers and integrees and to specially approved other Second Party personnel, as noted below. USCS organizations that wish to sponsor Second Party personnel for direct access to NSA/CSS ISs shall:

a. (U) Acquire and maintain, for each Second Party candidate, a record of the information specified within the Annex;

b. (U) For integrees only, prepare a formal requirements statement describing the systems, information, and services required for the Second Party individual(s) to perform official NSA/CSS-sanctioned duties; and

c. (U) Forward the sponsor and candidate information described in the above subparagraphs a (and b when applicable), to the Second Party and Multinational Affairs Division (P523) for approval and subsequent transferal to the Office of Security and Counterintelligence (A5) for NSA/CSS Personnel Security System Database (e.g., CONCERTO) record development. Service Partners will forward sponsor and candidate information through their respective cryptologic offices at NSAW (NSA/CSS Washington).

24. (U) **Exceptions to Access Policy:** Organizations requesting an exception to this policy or its annex shall coordinate a written request with their Information System Security Officer (ISSO). Requests will be reviewed by the Information System Security Manager (ISSM) and Second Party and Multinational Affairs Division (P523), prior to submission to the NSA/CSS Authorizing Official (AO) for decision.

**(U) RESPONSIBILITIES**

25. (U) USCS organizations sponsoring Second Party personnel for direct NSA/CSS IS access and NSA/CSS accounts shall:

a. (U) Verify that formal access requirements, including requirements for ISs, data, and services, are defined for Second Party personnel and appropriately coordinated with other organizations when access to data from multiple information stewards is required;

b. (U) Ensure that access requests are consistent with requirements for performance of official NSA/CSS-sanctioned duties;

c. (U) Advise the Second Party and Multinational Affairs Division (P523) and Service Cryptologic Offices (if applicable) of the formal access request requirement and obtain Second Party and Multinational Affairs Division (P523) concurrence;

d. (U) Confirm that the sponsored Second Party personnel are registered in the NSA/CSS Personnel Security System Database (i.e., CONCERTO) and the NSA/CSS Directory Service (i.e., SEARCHLIGHT);

e. (U) Verify that the Capabilities Directorate (Y) has approved all connectivity and access mechanisms before granting Second Party data access;

f. (U) Notify the Second Party and Multinational Affairs Division (P523), respective Service Cryptologic Offices (if applicable), the ISSO, the manager of the controlled interface, and system administrators when Second Party personnel access is no longer required;

g. (U) Be accountable for Second Party direct system access. Report any suspected anomalies, known or suspected unauthorized access, or problems associated with sponsored Second Party access in accordance with NSA/CSS Policy 6-23, "Reporting and Handling of NSA/CSS Information System Security Incidents" (Reference k); and

h. (U) Report anomalous activity and incidents to the Office of Security and Counterintelligence (A5) and the Capabilities Directorate (Y) for appropriate investigation.

26. (U) The Capabilities Directorate (Y) shall:

a. (U) Establish and maintain central oversight and accountability for Second Party access through the controlled interface and its separate services; and

b. (U) Provide technical guidance on quality, technical risk assessment, and procedures for connecting any Second Party personnel to NSA/CSS classified ISs.

27. (U) The Second Party and Multinational Affairs Division (P523) shall:

a. (U//~~FOUO~~) Ensure that appropriate NSA/CSS elements such as Capabilities Directorate (Y) and the Office of Security and Counterintelligence (A5) receive information relative to the arrivals and departures of Second Party persons sponsored for Direct NSA/CSS IS access/NSANet accounts. This will enable Standard Identification (sid) creation, SEARCHLIGHT record/account development/deletion as appropriate, and PKI approvals. These database records will form the core information set to enable NSA/CSS to satisfy internal, Department of Defense, and Intelligence Community requirements for secure and discrete information access and exchange; and

b. (U//~~FOUO~~) Approve the creation of NSANET accounts for Second Party Personnel eligible for direct access.

28. (U) The Security and Counterintelligence (A5) shall:

a. (U//~~FOUO~~) Receive and review approved requests from the Second Party and Multinational Affairs Division (P523) for Direct NSA/CSS IS access/NSANet accounts by Second Party persons and develop and maintain appropriate security records (e.g., CONCERTO) and convey sid and record data to Capabilities Directorate (Y) directorate systems that support and mediate such access (e.g., SEARCHLIGHT, CASPORT); and

b. (U) Investigate anomalous activity and incidents associated with Second Party access to NSA/CSS classified ISs in coordination with the NSA/CSS Capabilities Directorate (Y).

29. (U) The NSA/CSS Headquarters and Field ISSMs shall work with USCS organizations sponsoring Second Party integrees to ensure that information system security issues are addressed and resolved.

30. (U) NSA/CSS AO shall review requests for exceptions to this policy and render decisions.

31. (U) Privileged access users and ISSOs shall:

a. (U) Notify USCS system users when Second Party personnel have accounts on an IS or local area network;

b. (U//~~FOUO~~) Confirm that Second Party accounts are set up correctly and removed upon completion of specified official duties per NSA/CSS Policy 6-8, "Information System User and Supervisor Security Responsibilities" (Reference l);

c. (U) Report any anomalous activities in accordance with Reference k and assist, as necessary, in any investigations or analyses of such anomalies; and

d. (U) Assist in the enforcement of the data access procedures established by the information steward's or sponsor's policies and directives.

**(U) REFERENCES**

32. (U) References:

a. (U) U.K.-U.S. Communications Intelligence Agreement (UKUSA) dated 5 March 1946.

b. (U)



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

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

c. (U) NSA/GCHQ/DSD/CSE/GCSB Second Party Intranet Connection MOU dated 27 October 1998.

d. (U) [Redacted]

e. (U) Intelligence Community Directive 503, "Intelligence Community Information Technology Systems Security Risk Management," dated 21 July 2015.

f. (U) SID Management Directive (SMD) 421, "United States SIGINT System Database Access," revised 25 March 2008.

g. (U) SID Management Directive (SMD) 422, "USSS Mission Delegation," revised 15 April 2008.

h. (U) SID Management Directive (SMD) 427, "Access to Classified U.S. Intelligence Information for Second Party Personnel," revised 28 December 2013.

i. (U) SID Delegation of Approval Authorities Matrix dated 20 November 2014.

j. (U) IAD Management Directive 128, "Approval and Release of Technical IA Information," dated 22 June 2012.

k. (U) NSA/CSS Policy 6-23, "Reporting and Handling of NSA/CSS Information System Security Incidents," dated 4 December 2012 and revised 14 November 2014.

l. (U) NSA/CSS Policy 6-8, "Information System User and Supervisor Security Responsibilities," dated 1 August 2016.

**(U) DEFINITIONS**

33. (U) Authorizing Official (AO) – A senior (Federal) official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation. (Source: CNSS Instruction (CNSSI) 4009 dated 6 April 2015)

34. (U) Cryptologic – Related to the collection and/or exploitation of foreign communications and non-communications emitters, known as SIGINT; and solutions, products, and services to ensure the availability, integrity, authentication, confidentiality, and non-repudiation of national security telecommunications and information systems, known as Information Assurance (IA). (Source: NSA/CSS Corporate Policy Glossary)

35. (U) Exception – Indicates that an implementation of one or more security requirements is temporarily postponed and that satisfactory substitutes for the requirement(s)

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Policy 6-20

Dated: 31 March 2014

may be used for a specified period of time. This is in contrast to a waiver that implies a security requirement has been set aside and need not be implemented at all.

36. (U) Global Enterprise Leaders – NSA/CSS Directors, the NSA Chief of Staff, SCC Commanders, Senior NSA/CSS Representatives, and the military commanders/civilian chiefs of NSA/CSS Extended Enterprise sites. (Source: NSA/CSS Corporate Policy Glossary)

37. (U) Information System (IS) – Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition/collection, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data, and includes software, firmware, and hardware. IS examples are: stand-alone systems, Local Area Networks, supercomputers, process control computers that perform special purpose computing functions (e.g., Supervisory Control and Data Acquisition, other Industrial Control Systems, embedded computer systems), and the communications networks that disseminate information. (Source: NSA/CSS Corporate Policy Glossary)

38. (U) Information Steward – An agency official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, collection, processing, dissemination, and disposal. (Source: CNSSI 4009)

39. (U) NSA/CSS Classified Network (NSANet) – The TS/SCI information technology that enables the NSA/CSS to conduct its cryptologic missions, including signals intelligence and information assurance, and to support cyber operations missions in concert with the NSA/CSS Global Cryptologic Enterprise. Several conditions must be satisfied before an IS can be considered part of the NSANet. In particular each and every IS that is part of the NSANet must have a registered unique IP address; must be located in a SCIF [sensitive compartmented information facility] accredited by NSA/CSS or another IC agency or a Second Party Partner and approved by NSA/CSS to conduct NSA/CSS activities; and be under NSA/CSS authority. (Source: NSA/CSS Corporate Policy Glossary)

40. (U) NSA/CSS Washington (NSAW) – NSA/CSS facilities at the Fort Meade, Friendship Annex (FANX), and associated campuses [Finksburg, Kent Island, and all leased facilities in the Baltimore/Washington metropolitan area]. (Source: NSA/CSS Corporate Policy Glossary)

41. (U/~~FOUO~~) Nuclear Command and Control IA Material (NCCIM) – IA materials used in safeguarding and validating the use of nuclear weapons and weapon systems. These include, but are not limited to materials used in authentication, encoding/decoding, and/or locking/unlocking functions associated with the command and control of nuclear weapons. (Source: NSA/CSS Corporate Policy Glossary)

42. (U) Privileged Access (PRIVAC) – A special access above those privileges required for the normal data acquisition or operation of an agency information system. PRIVAC is granted to the following types of users:

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

a. (U) Users having “super-user,” “root,” “administrator,” or equivalent special access to a system (e.g., systems administrators, computer system operators, system security officers, webmasters). Those individuals who have near or complete control of the operating system of the machine or information system, or who set up and administer user accounts, authenticators, and the like;

b. (U) Users who have been given the power to control and change other users’ access to data or program files (e.g., application software administrators, administrators of specialty file systems, database managers, administrators);

c. (U) Users having access to change control parameters (routing tables, path priorities, addresses, etc.) on routers, multiplexers, and/or other important components; and

d. (U) Users who have been given special access for troubleshooting of information system security monitoring functions. (Source: PRIVAC website (“go privac”))

43. (U//~~FOUO~~) Second Party – Any of these countries: Australia, Canada, New Zealand, and the United Kingdom.

44. (U) Second Party Headquarters Personnel – Second Party personnel who work at Government Communications Headquarters (GCHQ), Communications Security Establishment (CSE), Australian Signals Directorate (ASD), or Government Communications Security Bureau (GCSB) headquarters or field elements and who have a valid need to access NSA/CSS classified ISs and for whom an NSA/CSS sponsor is identified.

45. (U//~~FOUO~~) Second Party Integree – Second Party personnel integrated into an NSA/CSS or United States Cryptologic System element who, when integrated into an NSA/CSS environment, are working solely under the direction and operational control of the DIRNSA/CHCSS to conduct cryptologic or information assurance activities that support the NSA/CSS mission in accordance with NSA/CSS authorities, rules, and regulations. Integrees may be civilian or military Second Party SIGINT or IA personnel but may not be contractors; an individual from one of the Second Party cryptologic entities assigned to work for NSA/CSS, under DIRNSA/CHSS authorities. Duties associated with an Integree’s position shall be performed in support of the NSA/CSS mission and in compliance with Executive Order 12333, “United States Intelligence Activities,” as amended. (Source: NSA/CSS Corporate Policy Glossary)

46. (U) Second Party Liaison Officers – A government official from a Second Party country, either military or civilian, who works in support of his or her country’s objectives at a USG organization or installation. These individuals generally act as the immediate point of contact for official interaction between USG and the 2P for that geographic location. (Source: working definition, IC ITE and 5-Eyes Partner Fact Sheet, June 3, 2015)

47. (U) Service Partners – Those organizations with the five armed services that operate under Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS) authority, or joint members of the larger Unified Cryptologic System, but that are not part of the CSS (e.g., Army Corps, Division, Separate Brigade and Armored Cavalry Regiment or Navy Fleet SIGINT assets that are normally under SIGINT Operational Tasking Authority (SOTA) of a tactical commander). (Reference j)

48. (U) System Security Plan (SSP) – The formal document prepared by the information system owner (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan. (Source: CNSSI 4009)

49. (U) United States Cryptologic System (USCS) – The various U.S. Government entities tasked with a SIGINT mission, i.e., the collection, processing, and dissemination of SIGINT, or with an information assurance mission, i.e., preserving the availability, integrity, authentication, confidentiality, and nonrepudiation of national security telecommunications and information systems. (Source: NSA/CSS Corporate Policy Glossary)

50. (U) USCS Personnel – United States Government personnel who derive their authority to direct and conduct cryptologic operations (SIGINT and IA) from the Director, NSA/Chief, CSS (DIRNSA/CHCSS). USCS Government personnel can be defined in three categories:

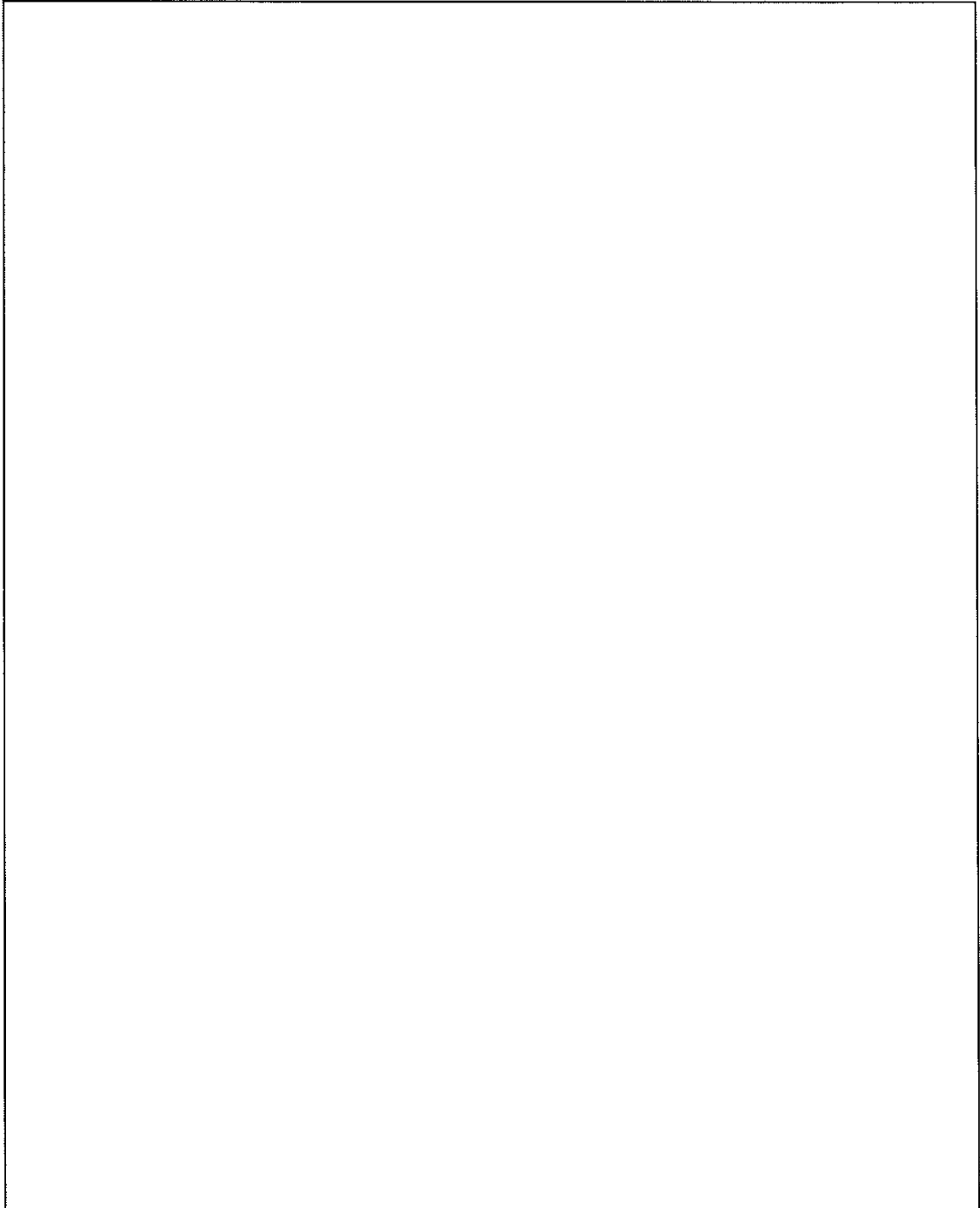
- a. (U) Civilian employees of the National Security Agency;
- b. (U) Military personnel and service civilians of the Service Cryptologic Components; and
- c. (U) Military personnel and service civilians of the non-CSS military organizations and civilian integrees from other U.S. Intelligence Community agencies who are considered members of the USCS when performing SIGINT or IA operations under the direction, authority, and control of DIRNSA/CHSS. (Source: NSA/CSS Corporate Policy Glossary)



~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~

Policy 6-20

Dated: 31 March 2014



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

Annex to Policy 6-20  
Dated: 31 March 2014

A-1

~~UNCLASSIFIED//FOR OFFICIAL USE ONLY~~