Ms. Scarlet Kim  
Privacy International  
62 Britton Street  
London, Great Britain

Dear Ms. Kim:

I refer to our letter, dated September 21, 2018, regarding the release of certain Department of State material under the Freedom of Information Act (the “FOIA”), 5 U.S.C. § 552. The Department has processed 21 additional responsive documents to your request. We have determined that 7 documents may be released in part and 14 documents must be withheld in full.

An enclosure explains the FOIA exemptions and other grounds for withholding material. Where we have made excisions, the applicable exemptions are marked on each document. In some cases, two or more exemptions may apply to the same document. All non-exempt material that is reasonably segregable from the exempt material has been released. The 14 documents withheld in full were withheld pursuant to FOIA Exemptions 1, 3, 5, and 6 U.S.C. §§ 552 (b)(1), (b)(3), (b)(5), and (b)(6). All released material is enclosed.

This completes the processing of your request. If you have any questions, you may contact Trial Attorney Marcia Sowles at marcia.sowles@usdoj.gov or (202) 514-4960. Please refer to the case number, F-2016-17168, and the civil action number, 17-cv-01324, in all correspondence about this case.

Sincerely,

Susan C. Weetman,  
Chief, Programs and Policies Division  
Office of Information Programs and Services

Enclosures: As stated
The Freedom of Information Act (5 USC 552)

FOIA Exemptions

(b)(1) Information specifically authorized by an executive order to be kept secret in the interest of national defense or foreign policy. Executive Order 13526 includes the following classification categories:

1.4(a) Military plans, systems, or operations
1.4(b) Foreign government information
1.4(c) Intelligence activities, sources or methods, or cryptology
1.4(d) Foreign relations or foreign activities of the US, including confidential sources
1.4(e) Scientific, technological, or economic matters relating to national security, including defense against transnational terrorism
1.4(f) U.S. Government programs for safeguarding nuclear materials or facilities
1.4(g) Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to US national security, including defense against transnational terrorism
1.4(h) Weapons of mass destruction

(b)(2) Related solely to the internal personnel rules and practices of an agency

(b)(3) Specifically exempted from disclosure by statute (other than 5 USC 552), for example:

| ARMSEXP | Arms Export Control Act, 50a USC 2411(c) |
| CIA PERS/ORG | Central Intelligence Agency Act of 1949, 50 USC 403(g) |
| EXPORT CONTROL | Export Administration Act of 1979, 50 USC App. Sec. 2411(c) |
| FS ACT | Foreign Service Act of 1980, 22 USC 4004 |
| INA | Immigration and Nationality Act, 8 USC 1202(f), Sec. 222(f) |
| IRAN | Iran Claims Settlement Act, Public Law 99-99, Sec. 505 |

(b)(4) Trade secrets and confidential commercial or financial information

(b)(5) Interagency or intra-agency communications forming part of the deliberative process, attorney-client privilege, or attorney work product

(b)(6) Personal privacy information

(b)(7) Law enforcement information whose disclosure would:
- (A) interfere with enforcement proceedings
- (B) deprive a person of a fair trial
- (C) constitute an unwarranted invasion of personal privacy
- (D) disclose confidential sources
- (E) disclose investigation techniques
- (F) endanger life or physical safety of an individual

(b)(8) Prepared by or for a government agency regulating or supervising financial institutions

(b)(9) Geological and geophysical information and data, including maps, concerning wells

Other Grounds for Withholding

NR Material not responsive to a FOIA request excised with the agreement of the requester
(U) Subject: NSA Intelligence Relationship with the United Kingdom

(U) Introduction:

(SEC/REL TO USA, GBR) The US/UK cryptologic relationship is the oldest and most productive of NSA’s foreign partnerships. It is based on a formal agreement (known as UKUSA) signed in 1946 by the predecessors to NSA and the Government Communications Headquarters (GCHQ), the UK’s National SIGINT and Information Assurance Authority. Mr. Iain Lobban is the Director of GCHQ and he leads a workforce of 2,000.

[Year: 2011-2012]

(SEC/REL TO USA, EVEY) GCHQ continues to strengthen its ties and improve coordination with other intelligence partners within the UK: the Secret Intelligence Service (SIS), an approximate counterpart to the CIA; the British Security Service (BSS), an approximate counterpart to the FBI; and the Defence Intelligence Staff (DIS) of the UK Ministry of Defence (MODUK), which directs and coordinates the activities of the intelligence units of the British military services.

(U/FOUO) The Special United States Liaison Officer, London (SUSLOL), a senior NSA civilian, guides the continued success of the UKUSA relationship in the UK. He serves as Deputy SUSLOL and is resident at GCHQ Headquarters in Cheltenham.

(U) Key Issues:

(U/FOUO) The UK Parliament recently passed legislation (known as the Justice and Security Act (JSA)) that is intended to better protect sensitive intelligence material (including that of the US IC) from public disclosure in civil lawsuits. The legislation was largely driven by the 2008 UK court-ordered release of classified CIA information in the Binyam Mohamed case. The JSA allows for closed proceedings in civil cases that implicate sensitive, national security material and exempts the UK IC (and by extension, the US IC) from cases in which litigants allege the
UK Government was "mixed up" in a case the litigant is bringing in another country (e.g., allegations of rendition, drone strikes, etc.).

(TS//SI//NF) NSA has continued to work closely with GCHQ to examine one another's dissemination practices and study how an already robust information sharing environment can be improved. NSA has encouraged GCHQ to make more of its published end product reporting available to U.S. customers, just as NSA has made a large percentage of its reports available to UK recipients. NSA's efforts have resulted in some improvements which will likely lead to increased sharing of published intelligence in the future.

(U) Success Stories:

- 
- 
- 

Classified By

Derived From: NSA/CSSM 1:52
Dated: 20070108
Declassify On: 20300104
(U) Problems/Challenges with the Partner

(U) None at this time

(U) Prepared by: 963-5837

Classified By [Redacted]
Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20380101

TOP SECRET///SI//NOFORN
MEMORANDUM FOR THE ASSISTANT SECRETARY FOR INTELLIGENCE AND RESEARCH, DEPARTMENT OF STATE

SUBJECT: Allegations of UK COMINT Collection Against General Motors (U) - INFORMATION MEMORANDUM

We have been in contact with GCHQ regarding the 15 June Financial Times of London Article on Robert Maxwell. If in the routine course of SIGINT operations either GCHQ or NSA were to encounter information in violation of the UKUSA agreement, specific steps would be taken to remove the data from the database, thus precluding any violation of the agreement.

J. M. McCONNELL
Vice Admiral, U.S. Navy
Director, NSA/Chief, O

Copy Furnished:
SA/DCI/FIR - Ambassador Hugh Montgomery

CLASSIFIED BY NSA
DECLASSIFIED BY NASA
CLASSIFIED BY: NSA/CSSM 1232
DECLASSIFICATION ON: ORIGINATING AGENCY'S DETERMINATION REQUIRED

HANDLE VIA COMINT CHANNELS ONLY

SECRET
Early intelligence files implicated Robert Maxwell

By Jimmy Burns and Robert Peston in London

THE UK GOVERNMENT had intelligence information years before the collapse of Robert Maxwell's empire that suggested the late publisher was acting dishonestly.

Maxwell was not seen as a risk to national security and was therefore not an "intelligence target" as such.

But it is understood that information pointing to his questionable activities existed within the files of the security services from Maxwell's early days as a businessman.

The Financial Times has also learnt that a full intelligence report was prepared for the Joint Intelligence Committee (JIC) at the time of Maxwell's death off Gran Canaria on November 5 last year. The JIC, which is part of the Cabinet Office, coordinates and assesses information from Britain's intelligence services, including MI5 and MI6. Separately, a former JIC official has claimed that some data on Maxwell's more recent activities, gathered by the intelligence services from intercepted telephone conversations and faxes, were passed to the Bank of England in 1989.

The Bank is understood to have carried out an intensive search last week and can find no such information on its files. Its officials have no recollection of receiving such information.

Mr Robin Robison, who worked as an administrative officer for the JIC, claims that other major British and foreign companies, large but not exclusively in the defence field, routinely have had their telephone and telex intercepted.

The companies under surveillance, he says, included CEC Marconi, Lonrho, Rolls-Royce, and their foreign competitors, and General Motors of the US.

Mr Robison, whose job involved sorting signals intelligence from the Government Communications Headquarters (GCHQ) in Cheltenham, western England, the center which filters international communications, claims in a statement that while working for the JIC, he sorted raw intelligence on Maxwell.

"The sigint (signals intelligence) I saw in the autumn of 1989 included intelligence data on Robert Maxwell taken from telephone conversations and faxes intercepted in Israel and the Mediterranean, probably from his yacht the Lady Ghislaine."

The information, according to Mr Robison, centred on Maxwell's businesses and his overseas trips although he cannot recall what the reports said in detail.

He says the information was evaluated and distributed to top government officials including the prime minister's office and cabinet ministers.

Mr Robison, who resigned from the JIC at the end of 1989, says he sent some GCHQ data on Maxwell to an economic subsection of the committee which included a seconded Bank of England official and others.

Classified intelligence material about Maxwell protected by code words was also sent regularly in a van to another official at the Bank's City headquarters in central London, he says.

The middle ranking official named in Mr Robison's statement is understood to act as a post-box within the bank for sensitive information. The official receives confidential documents and passes them to Bank departments which may have an interest in the contents.

In normal circumstances, the Bank would not expect to receive any information on Maxwell, since the late publisher did not own any businesses regulated by the Bank.

If it had received such information, it would have been passed on to the industrial finance department under Mr Pen Kent or the banking supervision section under Mr Brian Quinn, both directors of the Bank. Neither department has been able to find any record of receiving such information.

The Bank of England is known to have received information passed to it by the intelligence services about the activities of the failed Bank of Credit and Commerce International (BCCI) and its links with international terrorists.

Maxwell, who was born in Czechoslovakia, had high-level contacts with several former top communist leaders. There are also suggestions that Maxwell was under surveillance by the Czech secret services.

Mr Robison, a Quaker, resigned from the JIC over what he believed was the increasing unaccountability of intelligence gathering and the potential for the misuse of power.

Mr John Major, the prime minister, has declared himself in favour of more open government. He has appointed Mr William Waldegrave as minister for "open government", and recently broke with Whitehall tradition by publicly naming the heads of MI5 and SIS (MI6).

Ivo Dawsay writes: The Cabinet Office refused to comment on the claims yesterday, insisting that Mr Robison was a "very junior administrations officer" who had worked on the JIC for a relatively short period. It did not, however, deny that such information might have been collated.

"This refers to intercepts which obviously are part of intelligence systems," an official said. "We never comment on those for security reasons."
COMINT Collaboration with Australia

The United States collaborates with Australia in communications intelligence activities in accordance with the government-to-government COMINT agreement between the U.S. and the UK. The Australian COMINT effort is under the direction of the Defense Signals Division (DSD) in Melbourne, which functions as a Commonwealth activity, staffed by personnel from the UK and New Zealand as well as Australia.

The U.S. COMINT relationship with Australia is extremely close. The National Security Agency has a small group of technical people working in DSD; the Australians maintain technical liaison at NSA. Exchanges of raw material and products are extensive within the area of Australian interests.
IN REPLY REFER TO:

To: INR
Through: INR/DDC
From: INR/DDC
Subject: Publicity on Facilities

Attached are a recent New York Times article on the facility at Alice Springs and the Australian article to which it refers.

One of the project officers, tells me there has been extensive press coverage in Australia and some pressing questioning of the Minister of Defense in Parliament.

In response to questions on the costs of the base the Minister of Defense indicated a figure of $13 million, which will about cover the bricks and mortar. In a later statement, cleared between the Department and, to back up statements made in Australia it was agreed that in answer to questions we would confirm the figure and note that

Aerospace Technology in one of its issues estimated cost of the facility at much too high, but this figure has since been bruited about in Australia as the "authoritative" one. The Ministry of Defense asked if we could provide a figure on cost of the equipment being installed. Found it difficult to come up with an accurate estimate but concluded that it would take about to equip the base. ARPA indicated that any figure above would be unrealistic as far as ARPA was concerned, so told its Australian contacts that

the embassy advised on general developments with respect to particularly on any matters that may have political impact.

I understand that the Prime Minister is cleared for RCI is checking the clearance status of the principal officers accompanying him.
Australians Question Purpose of Secret U.S. Space Facility

By ROBERT TRUMBULL

SYDNEY, Australia, Dec. 27

The U.S. space agency has launched a highly classified United States "space research" facility in Australia that is linked to an American institute of the same name. The facility, said to have cost $250 million, is at Pine Gap, 12 miles from Alice Springs, a town at almost 5000 feet above sea level.

The installation is expected to be a nuclear-powered satellite that will be aimed at the American continent and the Soviet Union.

The installation would require the expenditure of $250 million, according to Mr. Cooksey, who has made it clear that the U.S. government has decided to build such a facility because of the recent developments in nuclear weapons.

Mr. Cooksey, who is responsible for the installation, said that the installation would be a major factor in determining the course of the nuclear arms race. He said: "The installation is a major factor in determining the course of the nuclear arms race. It will enable us to launch nuclear missiles from a very short distance, and we will be able to launch them from a very short distance."
PINE GAP

By Robert Cocksey

For some years now Australia has been important to the U.S. in aero-space matters, including nuclear weapons systems. This does not mean that American bombers with nuclear payloads or missiles with nuclear warheads are based in Australia. Rather, especially in the missile age, tracking and communications stations are as essential to U.S. nuclear weapons systems as rocket and warheads, or the command post in the White House. In his recent book, The Australian-American Alliance, Dr. Gelber points out that Australia is already the largest single centre for American missile and space operations outside the U.S.: with its technological and logistic facilities, its political stability and external security, it is the most suitable place for such operations in the southern hemisphere. There are a number of American space-tracking stations in Australia, for example, the twin stations at Honeyeek Creek and Tidbinbilla near Canberra. Such stations are not only involved in satellite exploration of the moon or reception of programmes from Tel-Star, but also in controlling photo-reconnaissance ("spy in the sky") satellites and observing Soviet satellites and monitoring their communications.

Certainly the most important American installation now operational is the North-West Cape Communications Station, which was officially opened in September last year by the late Prime Minister and has since been renamed in his memory "The Harold E. Holt Communications Station" by President Johnson. Readers will not doubt recall the controversy and confusion within the A.L.P. over the station in the first half of 1963: there is an agreement between Australia and the U.S. providing for consultation, but this is rendered meaningless by an exchange of letters containing the understanding that consultation does not impinge on the U.S. control:


the station's main function is transmission by very low frequency of submerged Polaris submarines in the western Pacific and in the Indian Ocean, deployed against parts of the Soviet Union and against China of target information and, if so instructed. As it is well known, Polaris missiles and their Soviet equivalents are relatively inaccurate and cannot therefore be used in a counter-city strategy directed at centres of population and industry, unlike highly accurate ICBMs which can be used as well in a counter-force strategy directed at the other's missile sites. For both the U.S. and the Soviet Union, Polaris-type missiles constitute a second-strike capability (ICBMs are the "never-to-be-used" first-strike capability), virtually invulnerable in submerged nuclear-powered submarines, able to be launched even if there is a first-strike against their homeland. Thus, goes the conventional wisdom, the two Super Powers are in a relationship of mutual deterrence; and North-West Cape contributes to the U.S. capability and hence deterrence and therefore the stability of world politics—that is, if we assume total rationality in decision-making ignore technological change and forget the emergence of China as a nuclear Power (see A.Q., June, 1968, p. 100).

North-West Cape was the subject of persistent questioning from a few members of the Labor Opposition from September, 1960, until the Government made the station's main function clear early in 1963. Later the same month the A.L.P. held a Special Commonwealth Conference to decide on its policy towards the station. In May the agreement with the U.S. was signed and—unnecessarily in constitutional law but usefully for a defence election—was introduced into parliament as a bill, vigorously debated and, of course, passed. Pine Gap has led a much quieter life. From the early 1960s there have been rumours of an American military aero-space installation at this picturequeely named spot twelve miles south west of Alice Springs. On 9 December, 1966, the Minister for External Affairs and the American Charge d'Affaires signed an agreement regarding to the establishment of a joint defence space research facility (Australia-Treaty Series, 1966: No. 17); apart from placing the facility near Alice Springs, providing for joint operation by the Australian Defence Department and the Advanced Research Projects Agency (ARPA) of the U.S. Defense Department, and requiring stringent security measures, there is nothing of interest in the text of the agreement not contained in its title. Even so, three issues arise out of the agreement must be noted: firstly, the provision for joint operation makes no stipulation about actual control; secondly, the various American space-tracking stations in Australia relate not to ARPA but to the National Aeronautics and Space Administration (NASA); and, thirdly, ARPA is part of the Office of Defence Research and
Engineering, responsible for research and development of missile systems and for some aspects of their operation—the Director of this Office is Dr. John S. Foster Jr., who with four of the Deputy Directors visited Canberra for discussions with the Minister, senior officials and scientists of the Australian Defence Department from 29 September to 1 October of this year. Mr. Fairhall announced the project and the agreement 11 December, 1966; the Government made no attempt to bring the agreement before parliament, as a bill or otherwise.

Immediately after Mr. Fairhall's announcement, the Member for Alice Springs in the Northern Territory Legislative Council, Mr. C. Orr, telegraphed the then Prime Minister, Mr. Holt, expressing concern that in the event of world war Pine Gap could become a target for nuclear attack and consequently Alice Springs might be destroyed. In a question upon notice Senator Bishop (A.L.P.) asked Mr. Holt through the Minister representing him in the Senate if certain subsequent allegations made by Mr. Orr were correct: *inter alia*, that the co-operation of people in the Alice Springs district about making land available was sought on the understanding that a space research project was involved "... but in fact it was a United States defence project—a spy in the sky—and the biggest outside the United States of America..." The Prime Minister replied on 13 April, 1967, denying any deception of the people of Alice Springs, mentioning "defence space research facility" but stressing space research, and adding—perhaps innocently—that, chiefly because missiles would not be launched from the site, it would not be a target in time of war. The next reference in parliament to Pine Gap came on 2 May of this year from Mr. Barnard, Deputy Leader of the Federal Parliamentary Labor Party and Shadow Defence Minister. He cited an article in the American journal *Aerospace Technology* (12 February, 1968, p. 3) which stated that the facility would cost $US225m, described it as the most sophisticated military space installation outside the U.S. and suggested that it might play an important role in future American detection and interception of missiles—the article in fact referred to detection and interception of missiles forming part of the new being developed Soviet "fractional orbital bombardaent system" (FOBS—see below). Mr. Barnard noted that the cost was about three times that of the North-West Cape Communications Station. He attacked Mr. Fairhall for giving no indication of the significance of the facility; but for the defence correspondent of *The Australian Financial Review* reading the article and publishing its content, he added, the public would remain completely unenlightened about the significance of Pine Gap.

In a number of articles published in August, *The Australian Financial Review* attempted an exposé of Pine Gap, apparently to press the Minister for Defence to explain and justify the functions of the facility. The first most important article, under the by-line of Peter Robinson, who is the defence correspondent referred to by Mr. Barnard, appeared on 2 August as the main page one news item; it was taken up that afternoon by *The Sun* (Sydney), another newspaper in the Fairfax group, again as a front page story and also with an editorial headed "A right to know". Peter Robinson commented on the secrecy surrounding the project: that we the Pentagon had declined to give any information about Pine Gap as this was the prerogative of the host government, and suggested that inquiries should be addressed to the Department of Supply in Canberra. Supply denied any connection with the project and recommended a Department of Defence; and Defence refused to say anything. Nevertheless Peter Robinson was able to report that the facility occupied ten square miles and, although not yet operational, construction was almost finished and testing of equipment was underway. Its cost was understood to be more than $200m, of which Australia's outlay was about $70m, for acquisition of land, fencing and various minor public works. In the previous twelve months there had been a steady flow of prefabricated buildings, from the U.S. via Adelaide, through Alice Springs, more recently, highly sophisticated electronic equipment, including radar at computers, had passed through. On the site were two radomes, each about 150 feet in diameter, protecting sensitive tracking antennas; other installations included more than fifteen air-conditioned buildings house other sensitive electronic gear. The facility, he suggested, is involved in three major American space-defence projects: firstly, the "manned orbit laboratory" (MOL), designed to test man's capacity to live and work in lengthy periods in orbit, but with military implications for the control of orbital weapons; secondly, "spy in the sky" satellites for orbit detection to monitor from the U.S.; and thirdly, as already mentioned above, a anti-Soviet FOBS system. Peter Robinson concluded that the Pine Gap facility is of strategic importance to the U.S. but not to Australia. A editorial in his newspaper on 5 August, although highly critical of the Government, was quite so dogmatic:

*... it is surely inconceivable that other independent, democratic Governments in the Western alliance would quietly sign away to a U.S. defence project of which the public know nothing—or that any Opposition parties would permit them to do so. It is quite possible that Pine Gap may be of fundamental importance to the future of Australian defence, or that it will be of critical importance in maintaining the "balance of terror" which has so far maintained world peace. If this is so, however, nothing has been done to make the Australian public aware of the fact.*
Mr. Fairhall commented briefly on Peter Robinson's article the day it was published. He represented Pine Gap as an "experimental" and not an "operational" station, in which Australian and American scientists together investigate "upper atmosphere and space phenomena"; but he did not say that Pine Gap would remain experimental, nor did he go so much as mention any projects to be undertaken. On the question of cost, a Defence Department official stated in ambiguous terms that this was $1.13m. of which Australia was contributing $1.1m.; as The Australian Financial Review pointed out, this $1.13m. covered only fixed installations and not the extremely expensive electronic equipment which takes the cost to about $2.00m. Mr. Fairhall said much the same in the House on 22 August in response to a question without notice from Mr. Calwell—a question so inexpertly phrased as to appear like a "Dorothy Dixie".

That is all of significance on the public record in Australia about Pine Gap. Apart from the Government's refusal to explain and justify the functions of the facility, the sorriest aspect of the affair is the performance of the A.L.P. The agreement was announced two years ago yet, apart from Senator Bishop's and Mr. Calwell's questions, and Mr. Barnard's passing remarks, the facility and its functions have not been queried by the Opposition. Since early this year some of the science policy advisers to the Labor Party have from time to time discussed Pine Gap with front-bench members of the parliamentary party; these advisers, and others who believe in foreign and defence policy, have been especially active since The Australian Financial Review made an issue of Pine Gap in August. Front-benchers, including some conventionally labelled "Left Wing", have declined to take up this issue; they are unwilling even to place questions upon notice that go beyond asking about the cost of the facility—and no questions have appeared on House or Senate "Notice Paper" in 1968. This passivity can be attributed to the "North-West Cape syndrome" in the party.

Leaders of the parliamentary party plainly look back with horror on the Special Commonwealth Conference of March, 1963: the photograph of the then Leader and Deputy Leader, Mr. Calwell and Mr. Whitlam, waiting outside the Hotel Kingston in Canberra to learn of the conference's decision and the tag applied by the Liberal Party during the Federal Election campaign the following November to the delegates inside—"the thirty-six faceless men"; the narrow margin for a policy of qualified acceptance of the station by 19 votes to 17; and, above all, fear of the party being identified as against the American alliance, so providing the Government with a potent issue in a defence election. But, now that the leaders and deputy leaders in the House and the Senate are members of the Federal Executive and the Federal Conference, the "faceless men" tag cannot be applied, even if it did affect voting as distinct from reinforcing prejudice. Again, a graduated approach, with a series of probing questions on notice, the circulation of position papers to members of Caucus and of the state executives, and a carefully prepared speech in the House by the Leader could prevent the development over Pine Gap of the confusion that surrounded North-West Cape and so bedevilled the special conference. Further, public opinion over the North-West Cape Communications Station was in any event mixed and, indeed, not unlike the resolution of the special conference, however impracticable that might have been. In an Australian Gallup Poll taken in April, 1963, 60% favoured building the station, 11% opposed and 29% were undecided; but in June 65% opted for joint control of the station, 25% said that joint control would not work and 10% did not know; and, also in June, 71% chose the alternative that the U.S. should "get our consent first" before sending via the station a message that might involve Australia in war, 21% said "no need" and 8% did not know. Although in the House Elections of 30 November the A.L.P.'s share of first preference votes declined to 44.7% of the total vote from 46.7% on 9 December, 1961, the intuitions of politicians and journalists aside, there was no evidence that North-West Cape, the American alliance and defence generally were significant in voting behaviour. Besides, although surveys showed overwhelming support for the American alliance, this does not mean that Australians accept that the content of the alliance should be determined solely by the U.S. Even so, this is the de facto policy of the Federal Parliamentary Labor Party, at least over Pine Gap.

Although there is little on the record in Australia relevant to the functions of the facility at Pine Gap, there is a great deal in the American aero-space magazines:3 read in conjunction with cognate areas of the literature of International Relations, some interesting tentative conclusions emerge. It seems likely that the first U.S. space-defence facility at Pine Gap (the one of which there were rumours in the first half of the 1960s) was concerned with a project for an "orbital bombardment system", involving satellites carrying nuclear weapons in orbit around the earth which on signal can drop on appropriate targets; this first facility was probably designed to monitor such satellites on paths hard to control from North America. After analysis of the cost-effectiveness of the orbital bombardment system in comparison with ICBMs, it was abandoned by the former U.S. Defense Secretary, Mr. McNamara. And, under Article IV of the Outer Space Treaty, which was negotiated by the U.S. and the Soviet

---

3. See especially, "Aerospace Technology" (formerly "Technology Week", which incorporated "Missiles and Rockets"), "Aviation Week and Space Technology" and "Air Force and Space Digest".
Union and came into effect in October, 1967, signatories "... undertake not to place in orbit around the Earth any objects carrying nuclear weapons...". It seems that this first facility never went beyond experiments in satellite control.

The present Pine Gap facility, which one imagines incorporates the first, clearly can, like lesser aero-space stations, perform a number of functions. The "manned orbiting laboratory" (MOL) mentioned in Peter Robinson's article is certainly an ARPA project with military implications, although still very much in the experimental stage: in testimony before a Congressional committee last year, the Director of ARPA said that his agency was looking at the feasibility of any space-based ABM (anti-ballistic-missile) system. It may well be, as Robinson suggested, that "spy in the sky" satellites are to be monitored from Pine Gap. Of course, satellites of this kind are already monitored by other space-tracking stations in Australia. But there are now satellite ICBM detection systems that probably require more sophisticated equipment: one system now being deployed involves satellite-borne radar in communication with a computer detecting and identifying ICBMs from the cross-section signatures of their rocket plumes; in advanced development is a satellite ICBM early-warning system based primarily on infra-red sensing techniques. Even so, these new detection systems would not require a facility costing the $52.25bn mentioned in February this year by the reputable Aerospace Technology.

That magazine (12 February, 1968, p. 3) and Peter Robinson no doubt relying on this source, saw as the main function of Pine Gap involvement in a system for the detection and interception of Soviet FOBS. ICBMs follow a ballistic trajectory along a great circle route: for both the U.S. and the Soviet Union this means that ICBMs deployed against the other would follow a route across the North Pole region. In a "functional orbital bombardment system" ICBMs are fired in the opposite direction, on a great circle route across the South Pole region. The Soviet Union has been testing FOBS since September, 1966: Mr. McNamara announced this early in November last year. For the Soviet Union against the U.S. FOBS would have the advantage of surprise; the "ballistic missile early warning system" (BMEWS) would provide no warning for a FOBS attack from the South; and over-the-horizon radar would provide only three minutes warning, besides being subject to interruption during sunspot activity and relatively vulnerable to jamming. But Soviet FOBS would have two main disadvantages: firstly, decreased payload, although at three megatons, this would still be twice the payload of the U.S. Minuteman ICBM or Polaris; and, secondly, there is an increase in targeting error by a factor of three to four over normal ICBMs, so that Soviet FOBS could only be used against the U.S. in a counter-city strategy. Now the advantage of surprise is not a strategic gain unless in a counter-force strategy the surprise can be used to take out American ICBMs in their silo and also the communications station for Polaris submarines at Manta—the one at North-West Cape can be taken out by a standard ICBM; otherwise, the U.S. second-strike capability is launched and the result is mutual destruction—and if over-the-horizon radar is working, this might be activated even if there is no time for Presidential decision. There are two possible ways of increasing the accuracy of Soviet FOBS: one is by "inertial reference" within the FOBS vehicle, but the probability of targeting error is still high; the other is to set up a monitoring facility in Cuba—but this would surely lead to another October, 1962—or to station crawlers along FOBS approach routes in the Caribbean to perform this monitoring function.

The installation of BMEWS in Western Australia, islands of the British Indian Ocean Territory and East Africa would give the U.S. 45-60 minutes warning against an attack by Soviet FOBS on the South Polar route compared with 15-20 minutes for ICBMs fired on the traditional North Polar route. However, there is no evidence that such a system is being set up; instead, apparently realising that the Soviet FOBS is not yet an operational system, the U.S. is relying upon those two new satellite ICBM detection systems mentioned above that are in part monitored from Pine Gap. And advanced detection, of course, means that surprise is no longer possible: that is, unless the Pine Gap facility is taken out by a Soviet ICBM. Certainly, with North-West Cape, it no doubt has a high priority or Soviet target list in a number of contingencies; and this would be singularly unfortunate for Alice Springs—at least the North-West Cape Station is in a pretty much uninhabited area. As for interception of Soviet FOBS, data from the Pine Gap facility can be fed to the ABM system on Johnston Island, mainly consisting of Spartan missiles, and specifically designed for intercepting orbital weapons; the "light" ABM system not being set up around major American cities is of virtually no use for interception of FOBS, because until 1975 only Washington, D.C., will have ABMs capable of intercepting missiles from the South. For the future, there is the ARPA project that might lead to space-based ABM controlled from the Pine Gap facility: this would increase the importance of Pine Gap as a target to the Soviet Union and also make it a priority target for China when that country has a modest force of ICBMs in the mid-1970s.

There is one other function that the Pine Gap facility might well under
take; and the high cost does suggest that some other function is being undertaken. At the moment the U.S. can deploy only Polaris missiles in a counter-city strategy against China: ICBMs, following a great circle route over the North Polar region, must cross the Soviet Union and, without prior arrangement, this might lead to a certain embarrassment. But if the U.S. developed FOBs, it could launch missiles on a South Polar route against China. The Pine Gap facility could perform this function, more easily. Australian American FOBs could be employed in a counter-force strategy against China. The Pine Gap facility could perform this function, more particularly as it is equipped with four Cary spectrophotometers, \(^4\) which can enable the facility to pick up the missiles with precision, allowing standard monitoring equipment to take over and place them with accuracy on Chinese ICBM sites.

If this is so, then Australia is even more deeply involved in the U.S. nuclear weapons system. Chinese missile guidance systems are not yet very sophisticated: it might take four ICBMs with thermo-nuclear warheads to be certain of taking out Pine Gap—and if a westerly is blowing, these might be considerable radio-active fallout over Queensland. Then there is the possibility of China making hostages of our cities for Pine Gap, or attempting nuclear blackmail. And once the light ABM net in the U.S. can be penetrated by Chinese ICBMs, then the American deterrent is no longer credible for Australia. The U.S. would still control North-West Cape and Pine Gap, but might well not act if one of our major cities were threatened or destroyed.

Presumably Soviet and Chinese intelligence units read the American aerospace magazines—and more thoroughly than this writer; perhaps too, defence planners in the Soviet Union and China are well aware of the strategic options open to the U.S. By refusing to explain and justify the functions of the Pine Gap facility, as distinct from revealing secret technical details, the Government is not confusing possible enemies as much as its own electorate. The Government simply refuses to acknowledge the extent of Australia's involvement in U.S. nuclear weapons systems and thus, with the assistance of a weak-kneed Opposition, prevents public debate on the central issue of Australian foreign policy—more important than Australian involvement in the Vietnam War. The nuclear question is central to world politics, to the relations between states and the survival of peoples.

---

4 Even before Mr. McNamara left the Defence Department (there were reports that the U.S. was developing FOBs) he was thought to be interested in building a system ('A.Q.'). June 1964, p. 10). Since Mr. McNamara's departure these reports have become persistent.

5 An Australian scientific visiting Cary Instruments in California discovered that there were four Cary spectrophotometers near Adobe Springs. As there are expensive and very sophisticated, and there are only about 2,000 in existence, he expressed some astonishment. He was told they were in a military installation—no further information was given.

---

THE LETHAL KNIFE—
CHEMICAL AND BIOLOGICAL WARFARE

By Sydney D. Rubbo^1

Can man continue to benefit from Science and yet escape the abuses that now so large from its misuse? This is not a rhetorical question. Science is as neutral as a knife; it may be a blessing or a curse depending on the heart and mind of the man who holds it.

Not so long ago, the Reverend T. M., Hasburgh, President of the University of Notre Dame, U.S.A., said, "Although Science is neutral, scientists cannot be. We need only remember Nazi Germany, where great Universities allowed themselves to be prostituted to inhumanity in the name of moral neutrality... Those who feel concern should become more dedicated to establishing their bearings in their own scientific specialties and in society in general, helping to impregnate the world with intelligence and love. We must be men of courage, unashamed of our commitment, dedicated to justice, to the great human values, unafraid to speak out, whether it is popular or not, knowing where we stand and why."^2

It seems to me that this view elegantly expresses the position of responsible scientists throughout the world and explains my stand on C.B.W.—Chemical and Biological Warfare. Having quoted this philosophy, to which I adhere, I sincerely hope that this article shall be interpreted as a sincere comment on an ethical issue, untied to politics or territorial interests.

That C.B.W. must be listed as one of tomorrow's weapons is evidenced by such statements as: "A future war will be characterised by the massive use of air forces, various rocket weapons and various means of mass destruction such as atomic, thermonuclear, chemical and bacteriological weapons,"^3 and "In modern warfare the intentional production of

^1 Professor of Microbiology, University of Melbourne.
United States Department of State
Washington, D.C. 20520

RIP (B)(6)
C06469342

FACSIMILE TRANSMISSION COVER SHEET

Date 7/31/98  Pages transmitted: ___ plus cover

TRANSMITTED TO:  FAX NUMBER: 70118

NAME: _____________________________________________
ORGANIZATION: ______________________________________
TELEPHONE: _________________________________________
DESCRIPTION: _________________________________________

TRANSMITTED FROM:  FAX NUMBER: (202) 736-7541

NAME: L/T (B)(6)
TELEPHONE: X71936

COMMENTS: Case you haven't seen.

NOTE: This copier is designated as "unattended" and will receive documents 24 hours a day. You must let the receiving party know you are sending a document.
Her Excellency Mrs Genta Holmes
Ambassador
Embassy of the United States of America
YARRALUMLA ACT 2600

Madam,


The Government of Australia proposes that the Agreement be extended for a period of ten years from 16 November 1998 and thereafter remain in force until terminated. The Government of Australia further proposes that after this extension has been in force for a period of seven years, either Government may at any time notify the other in writing that it desires to terminate the Agreement in which event the Agreement shall terminate three years after such notice has been given.

If the foregoing proposals are acceptable to the Government of the United States, I have the honour to propose that this Note and your confirmatory reply thereto shall together constitute an Agreement between our two Governments concerning this matter which shall enter into force on the date that the Government of Australia notifies the Government of the United States of America that all domestic procedures as are necessary to give effect to this Agreement in Australia have been satisfied.

Accept, Excellency, the renewed assurances of my highest consideration.

Alexander Downer

ALEXANDER DOWNER
EMBASSY OF THE
UNITED STATES OF AMERICA

Canberra, June 4, 1998

No. 67

Excellency:

I have the honor to refer to your note dated 4 June 1998 which reads as follows:

"I refer to the Agreement between the Government of Australia and the Government of the United States of America relating to the Establishment of a Joint Defence Facility at Pine Gap done at Canberra on 9 December 1966, as amended and extended (hereinafter "the Agreement").

The Government of Australia proposes that the Agreement be extended for a period of ten years from 16 November 1998 and thereafter remain in force until terminated. The Government of Australia further proposes that after this extension has been in force for a period of seven years, either Government may at any time notify the other in writing that it desires to terminate the Agreement in which event the Agreement shall terminate three years after such notice has been given.

"If the foregoing proposals are acceptable to the Government of the United States, I have the honor to propose that this Note and your confirmatory reply thereto shall together constitute an Agreement between our two Governments concerning this matter which shall enter into force on the date that the Government of Australia notifies the Government of the United States of America that all domestic procedures as are necessary to give effect to this Agreement in Australia have been satisfied."

The Honorable
Alexander Downer, M.P.,
Minister for Foreign Affairs,
Parliament House,
Canberra.
I have the honor to confirm that the Government of the United States of America accepts the proposals contained in your Note and that your Note and this reply shall constitute an Agreement between our two Governments concerning this matter which shall enter into force on the date that the Government of Australia notifies the Government of the United States of America that all domestic procedures as are necessary to give effect to this Agreement in Australia have been satisfied.

Accept, Excellency, the renewed assurances of my highest consideration.

[Signature]

Australia
Australian Capital Territory
City of Canberra
Embassy of the United States of America

I, the undersigned consular officer of the United States of America, duly commissioned and qualified do hereby certify that the foregoing is a true and faithful copy of the original/certified copy exhibited to me the same having been carefully examined by me and compared with the said original certified copy and found to agree herewith word for word and figure for figure.

IN WITNESS WHEREOF I have hereunto set my hand and affixed the seal of the Embassy at Canberra, Australia this 6th day June of 1978

[Signature]
National Security Agency
Office of Foreign Relations, NSF
COUNTRY HANDBOOK
UNITED KINGDOM

COUNTRY PROFILE

UNCLASSIFIED

Capital: London
Official Language: English
Population: 58.5 Million (1996 est.)
Type of Government: Constitutional Monarchy
U.S./U.K. Relations: Full Diplomatic
Defense Budget: USD 35.1 billion (3.1% of GDP (FY95/96))
Demographics: Labor force is 28 million; services 62.8%, manufacturing and construction 25.0%, government 9.1%, energy 1.9%, agriculture 1.2% (June 1992)

CRYPTOLOGIC ORGANIZATIONS (U)

(FOOU) The Government Communications Headquarters (GCHQ) is the UK National SIGINT Authority, as well as the home of a fee-for-service INFOSEC organization, the Communications and Electronics Security Group (CESG). GCHQ falls under the ministerial authority of the Foreign Secretary and the Foreign and Commonwealth Office (FCO), and its policy guidance comes primarily from the London Signals Intelligence Board (LSIB). Key oversight is administered by the Parliamentary Intelligence and Security Committee, who reports annually to the Prime Minister.

Other intelligence partners within the UK include the Secret Intelligence Service (SIS - also known as MI-6) an approximate counterpart to the CIA, and the British Security Service (BSS -(also known as MI-5) an approximate counterpart to the FBI.

CONTENTS

Country Profile ............................. 1
Country Map ................................ 1
Cryptologic Organizations .............. 1
Cryptologic Relationship ................. 2
Partner Capabilities/Technologies ....... 2
Future Prospects & U.S. Goals .......... 4
Recommendations ........................ 4
Key Personalities .......................... 4

Declassified by NSA
Confirmed by D. Force
DOS Senior Reviewer
CRYPTOLOGIC RELATIONSHIP (U)

Background (U)

The U.S.-UK Cryptologic relationship is the oldest and most productive of NSA's foreign partnerships. It is based on a formal "UKUSA Agreement," signed in 1946, and includes numerous supporting agreements signed over the years with GCHQ. This agreement is the basis for comprehensive cooperation on SIGINT and, to a lesser extent, INFOSEC activities.

Key Elements of Cryptologic Relations (U)

Under the UKUSA Agreement, each side agrees to share all SIGINT-related information; the exchange is unrestricted except for those areas that are specifically excluded (e.g., U.S. ONLY information) at the request of either party.

NSA's and GCHQ's intelligence priorities are largely convergent and GCHQ's SIGINT collection and processing capabilities often complement our own.

The cryptomathematics exchange with GCHQ is at the heart of our INFOSEC relationship. GCHQ is highly capable in the field of cryptomathematics and many 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 an influential foreign partner in advancing INFOSEC policies in the international arena.

Official liaison representation is maintained at each national center and a significant number of intelligence officers, analysts and technicians, work at each others' facilities. This includes a small, but increasing contingent of GCHQ representatives at the Regional Security Operations Centers in Ft. Gordon, Georgia; Medina, Texas; and Kunia, Hawaii. The Special U.S. Liaison Officer, London (SUSLO London or SUSLOL) is appointed by the Director, NSA, with the approval of the Director of Central Intelligence (DCI) and the advice of the National Foreign Intelligence Board, as appropriate. SUSLO London is accredited from the DCI to the London Signals Intelligence Board (UK National SIGINT Policy Authority) and is the senior authority for all cryptologic liaison in the UK.

PARTNER CAPABILITIES/TECHNOLOGIES (U)
(FOUO) Other current initiatives include the following:

**ENCRYPTION POLICY (U):**

**PERSONNEL AND FACILITY INITIATIVES (U)**

(U) Readoption of Unions. The new UK Government lifted the 13-year ban on unions at GCHQ in May 1997. NSA was initially concerned about the impact this might have on GCHQ employees assigned to Menwith
Hill Station, but no major issues have surfaced. NOTE: While GCHQ employees are civil servants and can now belong to civil service unions, Secret Intelligence Service (SIS) and British Security Service (BSS) employees (plus some law enforcement personnel) are "Crown Servants" and are, therefore, barred from belonging to a union.

(U) Private Finance Initiative. GCHQ has undertaken a significant initiative to use private sector capital to achieve a major facilities upgrade and colocation of its Headquarters operations into a single site in the Cheltenham area.

FUTURE PROSPECTS & U.S. GOALS (U)

The U.S.-UK Cryptologic Relationship will continue to be broad and deep well into the 21st Century. The relationship continues to be viewed as the most enduring and comprehensive of foreign partnerships for both parties.

The most recent supporting agreement to the UKUSA partnership is a joint policy statement, signed by the Directors of NSA and GCHQ in December 1997, reaffirming both agency's commitment to maximize the exchange and sharing of information, and where that is not possible, to notify the other of those exceptions.

RECOMMENDATIONS (U)

GCHQ has demonstrated a willingness to invest in its relationship with NSA, and a strong link exists between NSA's Unified Cryptologic Architecture and GCHQ's program. NSA will continue to urge GCHQ to keep apace with the implementation of NCS-21, particularly as UK global requirements continue to virtually match those of the U.S.

PERSONALITIES (U)

UNITED KINGDOM (U):

Director, GCHQ (DIR)
Mr. Francis Richards

Director CESG (DC)
Mr. Andrew Saunders

Foreign Secretary/Foreign and Commonwealth Office
Sir Robin Cook

Chief, Defence Intelligence Staff
VADM Alan West

Ambassador to the U.S.
Sir Christopher Meyer

UNITED STATES (U):

Ambassador to the UK
Mr. Phillip Lader

Special U.S. Liaison Office, London (SUSLOL)
MEMORANDUM FOR STATE/INR (Attention: Mr. Richard E. Curl)

THRU: NSA/CSS REPRESENTATIVE STATE DEPARTMENT

SUBJECT: Technology Transfer Cooperation with Australia

A. Background

Australia is not a member of CoCom and has never been invited to participate directly. Nevertheless, an Australian Interdepartmental committee recommended in June/July 1984 that general CoCom guidelines be followed when license applications for export of Australian goods are being considered by the Australian Government. The Prime Minister accepted the committee's recommendation.

B. Current Action

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

Classified by NSA/CSSM 123-2
Declassify on: 0ADR

Handle via COMINT channels only
CONFIDENTIAL

Declassified by NSA
Confirmed by D. Pierce
Dos Senior Reviewer
C. Comment

Technical information will be limited to that necessary for DSO to perform its SIGINT and COMSEC missions. We believe these actions to be in accordance with existing SIGINT and COMSEC relationships with Australia.

D. Action Requested

(U) Your concurrence,

Chief
External Affairs

Approved by: Director of Policy, Mrs. Julia B. Wetzel

STATE/INR Determination:

_____ Concur

_____ Non-concur

HANDLE VIA COMINT CHANNELS ONLY
NSA Legal Opinion

(b) (5)
WASHINGTON, D. C.

29 June 1949

Mr. G. G. Creen
Chairman
Communications Research Committee
Ottawa, Canada

Dear Mr. Creen:

Your letter of 27 May 1949 was received and presented to USCIS at its regular meeting on 17 June 1949.

I am pleased to advise you of the acceptance, by USCIS, of the proposals set forth in your letter.

For the members of our Board, I wish to express the highest hope that the agreed arrangements will prove satisfactory and mutually beneficial to our future efforts in this field.

FOR THE UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD:

/s/ C. F. Cabell
C. F. CABELL
Major General, USAF
Chairman
Ottawa, Ontario  
27 May 1940

Major General C. P. Cobell,  
Chairman,  
United States Communication Intelligence Board,  
Washington, D.C.

Dear General Cobell:

During the past eighteen months a number of informal discussions have taken place between various members of the United States Communication Intelligence Board (USCIB), and members of the Canadian Communications Research Committee (CRC) concerning the present relations of the two bodies on Signals Intelligence matters. It has, I think, been the general view of United States officials that our mutual arrangements should be clarified.

2. We have accordingly given careful consideration to the matter, and we suggest that our arrangements should be set out in an exchange of letters between you, as Chairman of USCIB, and myself as Chairman of the Canadian CRC. I feel that the guarantee as to security can be equally well met in the same way.

3. I am therefore writing to you setting out the proposals which we feel would lead to satisfactory arrangements for both the United States and Canadian Communication Intelligence authorities.

4. The following arrangements are proposed by the Communications Research Committee of Canada representing all Canadian Communication Intelligence authorities which now function or may function in the future. If you agree with these arrangements, your agreement would similarly be on behalf of the United States Communication Intelligence Board representing all U.S. Communication Intelligence authorities which now function or may function in future.

5. Scope of these arrangements:

These arrangements will govern the relations of the above mentioned authorities in regard to Communication Intelligence which will be understood to comprise the unvaluated product, and all processes involved in the collection, production and dissemination of information, derived from the communications of countries other than the USA, the British Empire and the British Commonwealth of Nations. It is realized that collateral material is often required for technical purposes in the production, and the proposed arrangements for exchange of such material are dealt with separately in this letter.

6. Extent of Exchange of Information Related to Communication Intelligence:

The two Communication Intelligence authorities will exchange information on the basis indicated, provided such release is not considered by the producing authority to be prejudicial to its national interest.

[Handwritten note: NSA TS/REL, N.S. 50 01110, COPY NUMBER 27, PAGE 2 OF 2]
(a) Translations, notes and summaries will be exchanged on the specific request of each authority, or when determined by the producing authority to be of interest to the other:

(i) When necessary to meet the technical requirements of the Combat Centres for the accomplishment of the tasks which they are undertaking,

(ii) To meet the intelligence requirements of the agencies represented by each authority.

(b) Decrypts will be exchanged as required for technical aids.

(c) Intercepted traffic will be exchanged on the basis of Combat activities or requirements undertaken by the respective Combat Centres.

(d) Cryptanalysis

(i) All information regarding methods, machine aids, techniques and processes pertinent to the tasks undertaken by either Centre will be supplied to that Centre by the other.

(ii) Information regarding methods, machine aids, techniques and processes not specifically applicable to tasks undertaken by either Centre may be exchanged when such exchange is considered by both Centres to be in their mutual interest.

(e) Traffic Analysis and information on practices, procedure and equipment of foreign communication services

The full exchange of such information is required by Centres controlling intercept facilities in order to ensure the maximum efficiency and elasticity in the event of an emergency. All information necessary for making rapid changes in intercept assignments and its corollary Traffic Analysis will therefore be exchanged.

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

(b)(3)-P.L. 86-36
8. Channels between United States and Canadian Agencies

(a) USIC will make no arrangements in the sphere of Communication Intelligence with any Canadian agency except through or with the prior approval of Canadian CIC.

(b) The CIC will make no arrangements in the sphere of Communication Intelligence with any U.S. agency except through or with the prior approval of USIC.

10. Dissemination and Security

The term "collateral material" is defined as any material obtained from sources other than Communication Intelligence exploitation and which is applicable for technical purposes to Communication Intelligence operations. Any request for such material will specify the technical purpose for which it is to be used. Either authority may withhold collateral material when,

(a) it considers that exchange would be prejudicial to the national interest, or

(b) the Ministry, Department, Agency, office or person which originated the collateral material available, or which bears the responsibility for its control, has placed a limitation on its circulation.

11. Dissemination and Security

Communication Intelligence and technical matters connected therewith, which are SECRET or above, will be disseminated in accordance with security policy to be mutually agreed upon and kept under review by USIC and CIC. Within the terms of this policy, dissemination by either party will be made to U.S. recipients only as approved by USIC, and to Canadian recipients only as approved by CIC. Collateral material which is exchanged will be neither used by nor its existence revealed to others than the personnel of the Ottawa COMINT Centre and the Washington COMINT Centre without the specific consent in each case of the party supplying the collateral material.

12. USIC and CIC undertake not to reveal the existence of any of these arrangements, even in the most general terms, to anyone who is not indoctrinated in accordance with the agreed security policy, and then only to those who, by virtue of their official duties, require such knowledge.
13. Dissemination and Security -- Commercial

USCIC and CRC will ensure that without prior notification and consent of the other authority in each instance, no dissemination of information derived from Communication Intelligence sources will be made to any individual or agency, governmental or otherwise, that will exploit it for commercial purposes.

14. Previous Communication Intelligence Arrangements

These arrangements supersede the existing arrangements between Canadian and U.S. authorities in the Communication Intelligence field.

15. Alteration and Termination of these Arrangements

These arrangements may be altered completely or in part at any time by mutual consent. It is understood, however, that these arrangements may be terminated completely at any time on reasonable notice by either authority, should national interests require such action.

16. If these arrangements are satisfactory, I suggest that implementation should take place when you have notified me as Chairman of CRC that they are acceptable to your Board. Implementation can then be arranged by the Communication Intelligence authorities responsible to USCIC and CRC respectively.

17. In order to implement these arrangements as effectively as possible, each authority may establish liaison officers at the COMINT centres of the other authority with such freedom of action as is agreeable to the host authority.

18. I shall look forward to receiving notification from you that the arrangements set out in this letter are satisfactory to your Board.

Yours sincerely,

/s/ G. O. Cream
Chairman, Communications Research Committee
APPENDICES
FOR THE IMPLEMENTATION OF THE CANADIAN - U. S.
COMINT AGREEMENT

(Drafted at Canadian - U. S. Technical Conference - 7 - 13 November 1949)

(Revised at Canadian - U. S. Technical Conference - 11 - 14 April 1951)

TABLE OF CONTENTS

Introduction

Appendix A - Definition of Terms.

Appendix B - Principles of Security and Dissemination.

Appendix C - Emergency Planning.

Annexure A

Annexure B

Annexure C

Annexure D

Annexure E

Annexure F

Appendix D - Cooperation in Intercept Traffic Analysis and Exchange of Pertinent Materials and Information.

Appendix E - Cooperation in Cryptanalysis, and Exchange of Pertinent Materials and Information.

Appendix F - Cooperation in Translation, and Exchange of Pertinent Materials and Information.

Appendix G - Combined Communications.

Annexure A - Canadian - U. S. COMINT Communication Arrangements.

Annexure B - Communications for Re-located Activities.

Revised, April, 1951

- 1 -

TOP SECRET SUEDE
Appendix II / Exchange of Information on Intercept Equipment, Facilities, Production, Research and Development.

Appendix III / Exchange of Raw Traffic and Standardization of Raw Material Format.

Appendix IV / Liaison and Methods of Exchange of COMINT Materials and Information.

TOP SECRET SUEDE
APPENDICES

FOR THE IMPLEMENTATION OF THE CANADIAN-U.S.

COMINT AGREEMENT

INTRODUCTION

1. The following arrangements governing the collaboration between the U.S. and Canadian COMINT Agencies are in implementation of, and are appendices to, the Canada-U.S. COMINT Agreement of 29 June 1949. These Appendices were originally produced at the Canadian-U.S. Technical Conference, 7-11 November 1949. At the Canadian-U.S. Technical Conference, 11-14 April 1951, the following changes and additions were recommended: Appendix C was revised, and Annexures A through F were added; Appendix D was revised, and Annexures A and B were added. None of these arrangements shall be construed as contravening any clauses of that Agreement, but shall take effect within the scope and limitations established thereby.

2. In accordance with these arrangements, each party will furnish as a continuing and current basis such information related to Communication Intelligence as is pertinent to the tasks undertaken by the other party, subject to the provisions contained in para. 6 of the Agreement. In addition, each party may maintain liaison personnel at the Agency or Agencies of the other party.

3. The two parties will continue to effect such standardization, e.g., of technical terminology, layout, procedure and organization, as may be practicable.

4. By the close collaboration thus established, and by means of discussion, agreement, and arrangement as to changes to be made, the two parties will continue to effect elimination of undesirable duplication in order to assure the maximum exploitation of foreign communications. However, the activities undertaken by each party must be basically suited to its own needs and capabilities, and therefore neither is in a position to accept any formal and fixed commitments for the allocation of specific tasks to its respective Agencies. It is understood that an informal and flexible allocation of certain tasks is advisable, subject to alteration by either party at need and sometimes without prior notification. If any alteration of an informal allocation is cancelled it will inform the other party as soon as possible, and will make every effort to maintain the intercept coverage on the task surrendered if the party has been obtaining unique material.

5. It is agreed that each party will keep under review the problem of the provision of adequate COMINT telecommunication facilities and the associated problem of peak and routine for the passage of COMINT material of all kinds, and will take all reasonable steps toward further improvement.

Revised,
April, 1951
6. The two parties recognize the need for combined emergency plans ready to be put into operation at or before any outbreak of hostilities involving both parties. They have therefore gone into considerable detail in planning for re-location of threatened intercept stations.

7. Each party will provide the other with two or more copies of all reports mentioned in the following Appendices (and of like documents) which pertain to the agreed tasks undertaken by the other.

8. In the conveyance of any information in any manner by one party to the other, pursuant to the basic Agreement, the fact that the disclosing party may have the privilege of using a method or technique, or a device or apparatus pertaining thereto, on a royalty-free basis shall not of itself relieve the receiving party of the obligation to pay royalties.

9. All these implementing arrangements are subject to review and to modification by mutual agreement.

10. These implementing arrangements concluded at the 1951 Conference will become effective immediately after approval by both Communications Research Committee (CRC) and United States Communications Intelligence Board (USCIB).

NOTE: Appendices approved at the Canadian-U.S. Technical Conference 7-15 November 1949 and not mentioned here remain unchanged by the Canadian-U.S. Technical Conference, 11-14 April 1951.
APPENDIX A

DEFINITION OF TERMS

1. CHANNEL: A unit or sub-division of a circuit will be known as a channel.

2. CIRCUIT: A telecommunications system between two points will be known as a circuit.

3. COLLATERAL MATERIAL: Collateral material is any material obtained from sources other than Communication Intelligence exploitation which is applicable for technical purposes to Communication Intelligence operations.

4. COMINT (COMMUNICATION INTELLIGENCE): Refer Appendix B, para. 3.

5. COMINT AGENCY OR COMINT CENTER OR AGENCY where used in this document will be understood to mean a government body organized for and engaged directly in the collection and processing of foreign communications for intelligence purposes.

6. COMINT ITEM: Any item of Special Intelligence or of Traffic Intelligence which is distributed or released by a COMINT Agency will be known as a COMINT Item.

7. COMINT-SEN: A summary or commentary produced by a COMINT Agency based on related COMINT Items, which may interpret those items in the light of one another or of information from other sources, will be known as a COMINTSEN.

8. COMMENT: Information appended to COMINT Items either in expansion or elucidation, or in expansion of the information contained therein, will be known as a comment.

9. CRYPTO-INTELLIGENCE: COMINT produced or obtained which bears on foreign communications will be known as crypto-intelligence.

10. DECRYPT: A foreign communication which has passed through the stages of cryptanalysis and decryption and is in its original language prior to translation will be known as a decrypt.

11. DIGRAPH: A two character group will be known as a digraph.

12. EXTRACT: A translation in part only of a decrypt or plain text will be known as an extract.

13. GIST: A statement of the essential substance of a decrypt or plain text or an abridged version of a translated text or extract will be known as a gist.

14. HEADING: Communication instructions for the delivery of a foreign communication, such as call-signs, serial numbers, external addresses, delivery instructions, indications of priority, group counts, date/time of origin, etc., will be known as a heading.
APPENDIX A

15. **Language Equivalent**: A word or phrase and its proposed or agreed rendering in English as found in a Supplemental Glossary will be known as a language equivalent.

16. **Plain Text**: An unencrypted foreign communication will be known as a plain text.

17. **Position**: The total assemblage of equipment used as a unit for an interception or transcription purposes will be known as a position.

18. **Scanning**: The process of examining decrypts or plain texts to determine if they shall be issued and, if so, in what form and with what priority, will be known as scanning.

19. **SIGINT** *(Signal Intelligence)*: Synonymous with COMINT *(Communication Intelligence)*.

20. **Special Intelligence**: Refer Appendix B, para. 4.

21. **Supplemental Glossary**: A list prepared by a COMINT Agency containing the proposed or agreed renderings in English of words or phrases which, though appearing in Standard Dictionaries, have additional meanings not given in these dictionaries, and of words or phrases of which the meanings are not to be found in a Standard Dictionary, will be known as a Supplemental Glossary.

22. **Traffic Intelligence**: Refer Appendix B, para. 5.

23. **Translated Text**: A translation of a decrypt or plain text will be known as a translated text.

24. **Translator's Note**: A remark or remarks added to a translated text, extract or list by the translator, in expansion, clarification or annotation of his rendering of the text, will be known as a translator's note. (It differs from a "Comment" in that it should not bear upon the intelligence implications of the text.)
APPENDIX B

PRINCIPLES OF SECURITY AND DISSEMINATION

INTRODUCTION

1. These principles shall be the basis of all regulations for the security and dissemination of Communications Intelligence issued by or under the authority of NSIB or DCI and other appropriate authorities of the Governments of the two parties. The scope and phrasing of such regulations may vary in accordance with requirements of the parties, agencies, departments, and ministries to whom they are designed to apply, but all shall be in accord with these basic principles in every respect and shall observe the standards herein as a minimum. As an aid to uniform interpretation, each party shall forward all pertinent NSIB and DCI regulations and directives to the other for information.

2. Conservation of COMINT sources is of supreme importance and there is no time limit for their safeguarding. It is essential that the production, exploitation, and dissemination of COMINT, resultant intelligence, and related technical information and material be specially controlled as specified herein.

DEFINITIONS

3. Communications Intelligence

a. Communications Intelligence (COMINT) shall be construed to mean technical and intelligence information derived from foreign communications and communications systems by other than the intended recipient.

b. COMINT activities shall be construed to mean those activities which produce COMINT by the interception and processing of foreign communications passed by radio, wire, or other electromagnetic means, with specific exceptions stated below, by the study of foreign communications systems and by the processing of foreign encrypted communications, however transmitted.

EFFECTIVE 1 JULY 1959

SP-0110

NSA TDCNTR 366
COPY NUMBER 372-17
THIS DOCUMENT CONTAINS 37 PAGES
Interception comprises search, intercept, and direction finding. Processing comprises range estimation, transmitter/operator identification, signal analysis, traffic analysis, cryptanalysis, decryption, study of plain text, the fusion of these processes, and the reporting of results.

3. a. Foreign communications are defined as all communications except:

(1) Those of the Governments of the U.S. and the British Commonwealth.

(2) Those exchanged among private organizations and nationals, acting in a private capacity, of the U.S. and the British Commonwealth.

(3) Those of nationals of the U.S. and British Commonwealth appointed or seconded by their Governments to serve in international organizations.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
3.  'I' is tactical COMINT produced by units which are designated to provide close support for the Commanders of combat forces.

6.  COMINT and COMINT activities as defined herein shall not include:

   (1) Intercept and processing of unencrypted written communications, except written plain text versions of communications which have been encrypted or are intended for subsequent encryption.

   (2) Intercept and processing of press, propaganda and other public broadcasts, except for encrypted or "hidden meaning" passages in such broadcasts.

   (3) Certain operations conducted by U.S., Canadian, or Commonwealth security authorities.

   (4) Censorship.

   (5) The peacetime exercise of 'I' resources in NATO commands, which involves the interception, analysis and exploitation only of radio transmissions (albeit "foreign") on networks established or used for exercises within or between those commands, provided that:

      (a) 'I-type' information produced during the exercise or revealed in post-exercise analysis, and information about the 'I' resources involved, is adequately safeguarded by NATO security regulations parallel to those for wartime 'I' operations, and the U.S. and Canada retain the right to express their views to the Command concerned as to the adequacy of the security classification applied.

      (b) Techniques used in the production of exercise 'I' during the exercise do not exceed in complexity the COMINT techniques involved in producing Category II(X) COMINT as defined in Annexure II.

      (6) The interception and study of non-communications transmissions (ELINT).
TOP SECRET EYES ONLY

1. Types of COMINT

There are two types of COMINT: Crypt Intelligence and Traffic Intelligence. They are defined as follows:

a. **Crypt Intelligence** is that COMINT which results from cryptanalysis or decryption including the solution of speech and facsimile security systems.

b. **Traffic Intelligence** is that COMINT produced by all means except cryptanalysis or decryption of intercepted communications.

2. Categories

For purposes of security handling and control COMINT is divided into categories and sub-categories. (See Annexure III)

a. COMINT is assigned to one of the following three categories as agreed between USIS and DCS.

1) **Category III COMINT** is that COMINT the unauthorized disclosure of which would risk extremely grave damage to national interests and specifically to COMINT activities and which, therefore, requires handling under special rules affording the highest degree of security protection. It is classified TOP SECRET, and is designated by a distinctive codeword.

2) **Category II COMINT** is that COMINT the unauthorized disclosure of which would risk serious damage to national interests and specifically to COMINT activities, but for which a less rigid standard of security is adequate. It is classified SECRET and is designated by a distinctive codeword.

3) **Category I COMINT** is that COMINT the unauthorized disclosure of which would risk little or no damage specifically to COMINT activities and for which, therefore, normal security classification procedures may be used. It will be classified at least CONFIDENTIAL and will not be designated by a codeword.

b. As mutually agreed by USIS and DCS, separate sub-categories of COMINT may be established within Categories III and II in order to permit...
Differentiation in the processing, dissemination, exchange or use of material.

6. **Technical Material**
   Technical material is understood to mean data concerning:
   a. Cryptographic systems.
   b. Communications systems, procedures and methods.
   c. Methods and equipment designed for COMINT activities and
      information related to any of the above.

7. **Information related to COMINT or COMINT Activities** - That information,
   other than COMINT itself, which reveals, directly or by implication,
   the existence or nature of any U.S. or Canadian COMINT activity.

8. **COMINT Channels** - A method or means expressly authorized for
   handling or transmission of COMINT and information related to COMINT activities
   whereby the information is provided exclusively to those persons who are appro-
   priately cleared and indoctrinated for access to COMINT.

9. **Codewords**
   Codewords, as used herein, are designators assigned to identify
   the source as COMINT; to distinguish between the COMINT categories and
   sub-categories; and to facilitate the application of regulations for the
   dissemination and use of COMINT.
11. Proper Authority

The term "proper authority", as used herein, shall be the level of authority permitted to authorize usage of the several categories of COMINT during hostilities and in special and emergency situations. The determination to make these exceptions and the authority to grant these exceptions shall lie only with senior officers and officials at levels to be established by USIS and DCS.

12. Indoctrination

Indoctrination is instruction as to the nature of COMINT and the security regulations and practices which govern the handling of COMINT material and COMINT activities.

13. Debriefing

Debriefing is the process of reminding persons no longer authorized to have access to COMINT or COMINT activities that they continue to be bound by all security regulations pertaining thereto. The debriefing shall include cautions that there is no time limit on the requirement to maintain security and that public disclosure does not free the individual from his obligation.

14. Hazardous Activities

Hazardous activities are those which place a person in a position where he runs a substantial risk of being captured or otherwise subjected to interrogation.
ASSIGNMENT OF CONINT TO CATEGORIES

16. In assigning CONINT to Categories (see paragraph 5), the following considerations will apply:
   a. The difficulty of detection or interception to include:
      (1) Sensitivity of techniques employed in solution and exploitation.
      (2) Sensitivity of source of intercept.
      (3) Relationships to other CONINT.
   b. The advantages to be gained versus the risk of disclosure and consequent damage through utilization under a given category taking into consideration the following factors:
      (1) The potential loss of intelligence.
      (2) The extent to which the target country is capable of improving the security of the communications in question.
      (3) The security grading given to contents by the country originating the traffic involved.
      (4) How wide the dissemination of certain CONINT should be to permit essential use of the intelligence contained therein.
      (5) The capability of certain third-party CONINT groups to exploit the CONINT in question with the attendant security risks beyond the direct control of U.S. and Canadian authorities.

17. USIS and DCS shall have prepared and maintained in current status mutually agreed lists to indicate CONINT placed in the several categories and in such sub-categories as may be established.

CLASSIFICATION AND CODEWORDS

18. Separate and distinctive codewords shall be employed to designate Category III and Category II CONINT and each sub-category thereof.
Category I COMINT shall not be designated by a codeword. Codewords shall be replaced when in the opinion of either US or DS a requirement exists for a change.

19. Documents and Technical material which reveal actual or prognosticated success, progress, scale and direction of effort, or other sensitive details about the production of COMINT shall bear the classification or the classification and codeword appropriate to the highest category or sub-category of COMINT to which they relate and shall be handled accordingly, even though such documents and technical material may not contain COMINT as such.

20. Raw traffic (i.e., intercepted traffic showing no evidence of processing for COMINT purposes beyond sorting by clear address elements, elimination of unwanted messages and the inclusion of a case number and/or an arbitrary traffic designator) shall be classified not lower than CONFIDENTIAL, and is understood not to be any specific category of COMINT and need not be designated by a codeword.

21. Codewords. The fact that codewords are used to designate COMINT categories shall not be made known to non-indoctrinated persons nor shall these codewords be used in the presence of non-indoctrinated persons.

SECURITY

22. All persons, including intercept operators, to be assigned to duties involving categories of COMINT other than Category I shall be indoctrinated. Recipients of Category I COMINT only will not be indoctrinated. Producers of Category I COMINT only need not be indoctrinated.

23. Every effort shall be made to restrict the number of persons indoctrinated for COMINT to the essential minimum.

24. It shall be permissible for persons who have access only to a lower category or sub-category of COMINT to work within agencies or Centers in which there are located other persons engaged in the production or exploitation of a higher category or sub-category of COMINT, only so
Long as due precaution shall be taken (by providing segregated, secure areas or otherwise) to ensure that the activities and knowledge of such persons are confined to the COMINT material and activities to which they are authorized to have access.

25. Except as agreed by USIB or DCS, all persons to be assigned to duties involving COMINT shall be the subject of security investigation and clearance. As an aid to promoting uniform minimum standards of eligibility, each party shall inform the other of the standards prescribed by it for this purpose.

26. Under extraordinary conditions, as determined by USIB or DCS, it may be essential for an individual to take up duties involving COMINT before the requisite investigation can be completed. In such cases, the person concerned may be suitably indoctrinated on the authority only of senior officers or officials as designated by the respective parties. In all such cases, steps shall be taken to ensure that security investigations and clearances are completed as soon as possible after indoctrination.

27. All persons who have been indoctrinated for COMINT shall be debriefed when they no longer have the requisite need-to-know.

28. Each party shall ensure that complete lists of indoctrinated persons are maintained.

29. USIB and DCS shall keep each other fully informed of the approximate number of indoctrinated persons in each of the departments, ministries, agencies, and offices receiving COMINT, by category or sub-category where applicable.

30. No national of one party shall be permitted access to the COMINT organizations or to the Categories III and II COMINT of the other party, unless he has been approved by his parent organization or Board and has been properly indoctrinated. Such access shall be limited to the categories or sub-categories of COMINT agreed by his parent organization or Board.
31. Every effort shall be made to ensure that no person who has a knowledge of current value about COMINT, except recipients of Category I only, such that his capture or interrogation could be a substantial risk to the security of COMINT, shall be assigned to or engage in hazardous activities. All possible action shall be taken to discourage or prevent any individual with a knowledge of current value about COMINT, except recipients of Category I only, from engaging in hazardous activities in any unofficial capacity at any time. Security principles governing participation in hazardous activities are set forth in Annexure B2.

32. Collection, processing, and dissemination of COMINT in exposed areas shall be undertaken only after a careful evaluation of the advantages to be gained and the risk to the security of COMINT. Security principles governing the conduct of COMINT activities in exposed areas are set forth in Annexure B2.

33. Except as implicitly involved in the operation of paragraphs 34-37, and 39 below, codeword material shall remain exclusively in the custody of indoctrinated persons, secure from examination by non-indoctrinated persons.

DISSEMINATION AND USE OF COMINT

34. General

a. The basic principle governing the dissemination of COMINT is the "need-to-know". Each item of COMINT shall, therefore, be made known only to those individuals who require it in the performance of their duties and, except as specifically provided in paragraphs 34d and 35-37 below, are indoctrinated and authorized to have access to the particular category or sub-category of COMINT to which such item appertains.

b. Except as specifically authorized by HSI or DCS, Category III or Category II (including sub-categories thereof) COMINT may be disseminated only to persons who have been cleared and indoctrinated for access to such material. Such persons may include nationals of collaborating British Commonwealth countries (U. K., Australia and New Zealand).
3c. Except as provided hereafter, no action which could compromise
the COMINT source may be taken on the basis of Category III or Category II
(including sub-categories thereof) COMINT.

3d. The need may arise, in individual cases of special sensi-
tivity, or more generally, for either party to handle COMINT items, or
information related to COMINT or COMINT activities, in a more restricted
manner than required by the provisions of this Appendix and its Annexures.
In such cases the other party will, on request, provide similar handling
for the specific items concerned.

(b)(1)
(b)(3)-50 USC 3024(l)
(b)(3)-P.L. 86-36
ASSIGNMENT OF COMINT TO CATEGORIES

16. In assigning COMINT to Categories (see paragraph 5), the following considerations will apply:
   a. The difficulty of solution or intercept to include:
      (1) Sensitivity of techniques employed in solution and exploitation.
      (2) Sensitivity of source of intercept.
      (3) Relationships to other COMINT.
   b. The advantages to be gained versus the risk of disclosure and consequent damage through utilization under a given category taking into consideration the following factors:
      (1) The potential loss of intelligence.
      (2) The extent to which the target country is capable of improving the security of the communications in question.
      (3) The security grading given to contents by the country originating the traffic involved.
      (4) How wide the dissemination of certain COMINT should be to permit essential use of the intelligence contained therein.
      (5) The capability of certain third-party COMINT groups to exploit the COMINT in question with attendant security risks beyond the direct control of U.S. and Canadian authorities.

17. USH and DCS shall have prepared and maintained in current status mutually agreed lists to indicate COMINT placed in the several categories and in such sub-categories as may be established.

CLASSIFICATION AND CODEWORDS

18. Separate and distinctive codewords shall be employed to designate Category III and Category II COMINT and each sub-category thereof.
provided the form of issue gives no indication whatever of the CKINIT origin.

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
36. c. The decision to execute the provisions of paragraphs a and b above shall be made only after a determination that the advantages to be gained clearly justify the risk of compromise of the source. Due regard shall also be given to:

(1) The relative value of the particular OKHINT source involved and the possibility that its compromise may lead to the loss of other OKHINT sources.

(2) The possible repercussions on current and future operations and also on other commands and areas.

d. In order to minimize the risk of compromise the following precautions shall be observed:

(2) A minimum number of non-indoctrinated personnel shall be given the information, and

(a) when practicable the information shall be so presented that it cannot be traced to OKHINT as a source, or

(3) The minimum amount of information necessary to justify the contemplated action shall be revealed.

e. If communications by electrical means are involved they must be enciphered in the most secure cryptographic system available.

f. If time permits the commander or official making this decision should consult with his supporting OKHINT authority for technical advice.

- 14 -
h. Sub-paragraph 35c above, applies with respect to emergency usage of the material in the sub-category of Category II described therein.

d. Sub-paragraph 36d, above, applies with respect to emergency usage of Category I CONINT.

37. Hostilities

a. It is recognized that in the event of hostilities certain material will be downgraded. In connection with the mutually agreed lists referred to in paragraph 17, USIB and DCS will agree upon types of materials suitable for downgrading during hostilities. When hostilities appear imminent or occur USIB and DCS will immediately consult upon downgrading measures to be taken.
f. Whenever any of the provisions of sub-paragraphs 7h and 7k, above, are executed, USIB and DCI will keep each other informed. This information shall contain a description of the OCHINT material involved, and, in general terms, the extent and nature of the action taken.

g. In the event of hostilities the proper authority may direct the appropriate OCHINT organization responsible for providing his support to downgrade to Category I that material in the sub-category of Category II described in paragraph 35g which is relevant to the situation. Such information may then be disseminated or action be taken therein in accordance with the procedures established for Category I OCHINT. The cognizant OCHINT organization will immediately, without prior consultation with higher authority, make available as Category I such material of this sub-category as is required. USIB and DCI will keep each other informed of downgrading actions taken.

h. Sub-paragraph 34d, above, applies with respect to wartime usage of Category I OCHINT. Whenever suitable 'T' channels are available, they will be used for this dissemination.

PROCEDURES

38. The appropriate classification and coding shall:

a. Appear on every sheet of paper which contains or discloses Category III or II OCHINT or a sub-category thereof, and be applied to documents and technical material as defined in paragraph 19. Except as provided in paragraphs 35-37, above, this rule applies to maps and charts on which are plotted data and information derived from these categories of OCHINT.
36. b. Be encrypted in the text of every encrypted communication conveying Category III or II COMINT and appear in plain language at the head of the decrypted version. This rule shall apply in all instances except as provided in paragraphs 35-37, above, and under the following conditions:

(1) COMINT organizations may, without encrypting the appropriate codeword in the encrypted text, transmit TOP SECRET and SECRET technical matter over cryptographic channels or ciphers expressly and exclusively provided for such technical matters.

(2) COMINT organizations and intercept or D/V stations may, at the discretion of the officer in charge and after full consideration of the risks involved to the source, omit the classification and the appropriate codeword from its work-sheets and similar documents used exclusively within each agency or station. The classification may be omitted from raw traffic passed between agencies or from intercept and D/V stations to agencies.

38. Category III COMINT and related technical material shall not be transmitted in plain language except as follows:

a. Sealed, by safe-hand channels, over routes specifically approved by USIB and DCS.

b. Over completely protected local communication systems exclusively internal to agencies or offices producing or utilizing COMINT.

c. Over landlines specifically approved in each instance by USIB or DCS.

40. Category II COMINT and related technical material shall not be transmitted in plain language except as provided in paragraph 39 above, or by protected postal channels internal to, or under exclusive control of, the U.S., Canada or other collaborating British Commonwealth countries.

41. Category I COMINT and related technical material should be transmitted by COMINT or ‘Y’ channels wherever possible, but may be transmitted by conventional channels used for intelligence material of similar classification.
It may be transmitted in plain language by a means exposed to interception only when there is no suitable means of secure communications available and when there is an urgent operational need to do so. Whenever possible such plain language transmissions should be in the form of operational orders so worded that the subject matter cannot be traced specifically to COMINT as its origin.

42. Raw traffic may be transmitted in plain language as provided in paragraph 35, above. Raw traffic classified CONFIDENTIAL may also be transmitted in accordance with the normal procedure for this classification, except that when transported across the territory of the country originating the traffic, it shall be with the express sanction of USD or DOS. This sanction will be granted only in cases of compelling need.

43. Except as provided in paragraphs 35-37, above:

a. Category III COMINT and related technical material transmitted in encrypted form shall be encrypted in special cryptographic channels expressly provided for these subjects.

b. Category II COMINT and related technical material transmitted in encrypted form shall be encrypted in special cryptographic channels expressly provided for these subjects, those listed in paragraph a., above, or in the most secure cryptographic channel available.

c. However, in the case of cryptographic systems mutually approved for the purpose, the transmission of COMINT, related technical material and raw traffic over the same channel is authorised, provided that such channels are reserved for these subjects exclusively.

44. In order to facilitate a concerted effort directed toward the determination and assessment of the causes and effects of known or presumed COMINT compromises or losses, it is agreed that:

a. Whenever any breach of its COMINT security regulations or any other circumstance which in fact has, or can be presumed to have, compromised COMINT or COMINT codewords, or to have revealed COMINT successes to unauthorised
persons, becomes known to either party, it shall inform the other by means of a report embodying the pertinent facts and conclusions in each case, except that when the party concerned concludes that there is a good reason to believe that such compromise or revelation has not reached and will not, in fact, reach foreign nationals, no report need be made to the other party.

b. Whenever a significant change occurs in foreign cryptographic or communications security, the party discovering such change shall notify the other. Each party shall then analyze and assess the known and suspected circumstances having a bearing upon the change; these analyses and assessments shall be exchanged by the parties; and each party shall thereafter keep the other fully informed of any additional information bearing upon the case.
APPENDIX B
ANNEXURE B1

THE ASSIGNMENT OF COMINT TO CATEGORIES AND SUB-CATEGORIES

1. This Annexure delineates the basis for (a) the establishment of sub-categories, (b) the assignment of COMINT to categories and sub-categories, (c) the classification of COMINT assigned to categories and sub-categories, and (d) the application of codewords to categories and sub-categories. This Annexure is not intended to accomplish the detailed categorization of all COMINT. However, along with the criteria described in Appendix B, it governs the preparation and maintenance of current, mutually agreed lists to indicate the precise assignment of all COMINT to categories and sub-categories.

2. Category 1 COMINT shall be classified CONFIDENTIAL, SECRET, or TOP SECRET as appropriate in accordance with national security classification procedures and shall not be designated by a codeword. It shall contain the following, provided that interpretations of material of higher categories are not included:

   c. Such COMINT from the less sensitive sub-category or category II as may be so assigned in accordance with Appendix B. (See paragraph 35h)

   d. Such additional COMINT as has been or may be specified and mutually agreed by USIA and DCS.

EFFECTIVE 1 MAY 1959

- 20 -
3. Category II COINTEL shall be classified SECRET and shall be
designated by a distinctive codeword. It shall contain all COINTEL not
otherwise assigned to Categories I or III or Sub-categories established
within Category II.
4. Category III COINTEL shall be classified TOP SECRET, and shall be
designated by a distinctive codeword. It shall contain:
   a. Crypt Intelligence derived from high-grade systems, in-
      volving the application of sophisticated cryptanalytic techniques, as
      specified and mutually agreed by USIB and DCS.
   b. Traffic Intelligence derived from messages or message
      headings encrypted in codes and ciphers of high security or complexity,
      as specified and mutually agreed by USIB and DCS.
   c. Traffic or Crypt Intelligence which reveals success against
      unusual, sensitive, or complex transmission procedures or devices.
   d. Material obtained from special sources or against targets
      considered by the procuring organization to be so sensitive as to warrant
      the protection afforded this category.

5. Other Crypt or Traffic Intelligence which USIB or DCS
by mutual agreement determine should be given the highest degree of
security protection because of the potential loss of intelligence which
would result from compromise.

5. Sub-categories of Category II shall be established as follows:

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
b. Sub-Category II(X) COMINT is that Category II COMINT which is considered less sensitive than other Category II COMINT and may, therefore, be given more extensive dissemination in order to provide for effective utilisation. It is classified SECRET and is designated by a distinctive codeword. It is this sub-category which is described in paragraph 35g of Appendix B. Provided that no information obtained from Categories II and III COMINT, such as complex changing callsign and frequency systems or unusual, sensitive or complex transmission procedures or devices, is included, this sub-category shall contain the following:

(1) Information derived from the following elements of foreign military, naval, air police, border guard and guerrilla communications or communications systems:

(a) Communications data
(b) Plain Text
(c) Any grid or zone references
(d) Cover Words
(e) Procedural codes used for brevity purposes
(f) Jargon codes

(2) Plain Text and associated communications data obtained from international commercial and foreign internal or external non-military circuits except that specifically assigned to other categories as mutually agreed by USIB or DCS.

(3) Such additional COMINT as may be specified and mutually agreed by USIB and DCS.
APPENDIX B

ANNEXURE B2

SECURITY PRINCIPLES GOVERNING THE CONDUCT
OF C marital operations in exposed areas

INTRODUCTION

1. It is recognized that effective interception of foreign communications and effective support of field commanders may require the establishment of C marital activities in locations which may suddenly fall under hostile control with consequent loss of C marital personnel and/or associated classified materials. It is agreed that, in addition to the pertinent, general provisions of Appendix B, the specific provisions which follow shall govern the conduct of C marital activities in such locations.

DEFINITIONS

(b)(1)
(b)(3)-50 USC 3024(i)
(b)(3)-P.L. 86-36
3. Hazardous activities as defined in paragraph 1A, Appendix B, include:
   a. Duties behind enemy lines, or in-shore operations off an enemy or unfriendly country.
   b. Flights over enemy or unfriendly territory unless on recognised corridor routes.
   c. Raids, minor formation attacks, underwater demolition operations, and service with a unit or formation forward of Division HQ.
   d. Duty in or visits to unfriendly countries and also other areas where time to time local conditions are considered to involve an unacceptable risk.

Safeguards for Assignment of Personnel to Hazardous Activities

5. As an aid to controlling assignment of personnel to hazardous activities, persons who are or have been indoctrinated will be divided into three groups:
   a. Group I - (Unrestricted)
      Individuals who are producers of Category I COMINT and have no knowledge of other Categories, or persons who, although indoctrinated for other Categories of COMINT, have so little access that they do not possess knowledge of current value, and are not subject to restrictions against hazardous activities.

   - 24 -
b. **Group F - (Minimum Restriction - one year)**

Individuals who have knowledge of current value about Categories II or III COMINT or their subcategories, who shall not be assigned to hazardous activities for a minimum period of one year following debriefing.

c. **Group F - (Permanent Restriction)**

Individuals with precise knowledge of COMINT processing techniques, competence or potential regarding the more sensitive Category III COMINT who shall not be assigned to hazardous activities at any time.

6. Exceptions to the above safeguards may be authorized by senior officers and officials at a level prescribed by HSIB or DCI. In considering such exceptions the protection offered by diplomatic status should not automatically be considered sufficient, but should be assessed in the light of the particular circumstances involved. In the case of Allied Command to which CANADA COMINT is provided through an SGO or CGO, the senior CANINT Indocminal U. S. and Canadian officials shall be authorized to make such exceptions.

**EVALUATION OF SITUATIONS IN EXPOSED AREAS**

7. The decision whether a given situation is risky or dangerous shall be made by HSIB or DCI or by such other authorities as are responsible for the security of the COMINT activities concerned, and shall be made in the light of the political, military, and other factors affecting the safety of the COMINT personnel and materials involved.

**FACTORS AFFECTING DECISIONS TO CONDUCT COMINT OPERATIONS IN EXPOSED AREAS**

8. COMINT operations shall be conducted in exposed areas only after due consideration of the COMINT losses which may result if the area concerned is suddenly attacked, and of the probable effect of such losses upon the conduct of COMINT activities elsewhere.
SAFEGUARDS FOR RISKY SITUATIONS

9. In the case of COMINT activities established in risky situations, the following safeguards shall be applied save as exceptions thereto are authorized by senior officers and officials at a level established by USIS or DCS:

   a. Only intercept, analytic and reporting tasks which cannot be performed satisfactorily in safe or protected situations shall be assigned.

   b. No Category III COMINT or related documents and technical material shall be held except those essential to the assigned task and of current application thereto, and the latter shall be maintained in such condition as to insure immediate destruction, if necessary, upon sudden threat of seizure.

   c. No person in Group P, as defined in paragraph 5a above, shall be assigned, unless required by technical considerations.

   d. Sufficient means of destruction shall be provided in order that complete destruction of classified COMINT materials may be carried out in the shortest time possible by the minimum number of personnel.

   e. Appropriate steps shall be taken to insure that adequate arrangements are made for safe evacuation of all personnel whose loss would be damaging and that the unit in question is kept informed of evacuation plans on a current basis.

SAFEGUARDS FOR DANGEROUS SITUATIONS

10. In the case of COMINT units established in dangerous situations the following safeguards shall be applied save as exceptions thereto are authorized by senior officers and officials at a level established by USIS or DCS:

    a. Only unique intercept tasks which cannot be accomplished elsewhere shall be assigned, and only such analysis as is locally required to support these tasks and permit essential technical reporting shall be performed.

    b. Only COMINT documents or technical aids essential and of current application to these tasks shall be held.

   - 26 -
c. No Category III COMINT or related documents and technical material shall be held.

d. Personnel technically informed in COMINT of a higher level or broader scope than is required for the limited mission of the unit should not be assigned if avoidable.

e. No person in Group M as defined in sub-paragraph 5b above shall be assigned unless his presence is vital for the effective functioning of the unit.

f. No person in Group P as defined in sub-paragraph 5c above shall be assigned in any circumstances.

g. Sufficient means of destruction shall be provided in order that maximum destruction of classified COMINT material may be carried on in the shortest time possible by the minimum number of personnel.

h. Appropriate steps shall be taken to insure that the unit in question is kept informed of evacuation plans on a current basis.
APPENDIX B

CLASSIFICATION AND HANDLING OF INFORMATION
RELATED TO CININT OR CININT ACTIVITIES

INTRODUCTION

1. This Annex establishes minimum standards with respect to the handling and classification of information which is neither CININT nor that contained in the "documents and technical material" as described in paragraph 19 of Appendix B, yet reveals, directly or by implication, the existence or nature of CININT or of CININT activities.

2. The nature of CININT and CININT activities and their susceptibility to loss require that certain information regarding these activities and their product be restricted to persons who have been cleared and indoctrinated for access to CININT. Certain other information concerning these activities and their product may be handled within conventional channels for information of similar classification. It is essential, however, that reference to the existence or nature of CININT or any CININT activity, either direct or indirect, be avoided except among those to whom the knowledge is necessary for the proper performance of their duties.

3. Information related to CININT or CININT activities which indicates a degree of success or progress in the production of CININT, a sophisticated CININT technique or the scale and direction of CININT effort to a degree which may stimulate countermeasures, as specified in Annex A hereto, must be safeguarded precisely as though it were CININT. Except as provided for hereinafter, documents containing such information, including messages transmitted electrically, shall be transmitted only via CININT channels, and shall bear the classification and CININT codeword appropriate to the most sensitive category or sub-category of CININT to which they relate.

4. Information related to CININT or CININT activities, specified in Annex B hereto, shall be kept exclusively within CININT channels, except as provided for hereinafter and in that Annex. Documents which contain such information,
including messages transmitted electrically, shall bear the appropriate classification but no COINHT codeword, and shall be clearly identified by the caveat "HANDLE VIA COINHT CHANNELS ONLY", stamped, typewritten, or printed on each page. In the case of bound documents, the identification will show on the cover and title page, if any.

5. Information pertaining to COINHT or COINHT activities, specified in Annex C hereto, may be handled in accordance with normal practice for other information of similar classification. However, nothing herein should be construed as prohibiting an authority from passing such information in COINHT channels. (In such cases, the caveat "HANDLE VIA COINHT CHANNELS ONLY" will not be used.)

SPECIAL USAGE

6. Should it become necessary to furnish information of the type listed in Annex A to non-indoctrinated persons, such action will be taken only after specific authorization in each case by proper authority designated by USIB or DCOS. When a document containing such information is released from COINHT channels, the codeword must be removed. NSA and CBHRC, through technical channels, will undertake to keep the other party informed, at least in general terms, of the material involved.

7. Information related to COINHT or COINHT activities of the types listed in Annex B may be furnished to non-indoctrinated persons, only with the prior approval of the originator or proper authority and in accordance with the procedures established by USIB or DCOS. When a document containing such information is released from COINHT channels, the handling caveat must be removed or rendered illegible.

8. Every reasonable precaution must be taken to ensure that documents released from COINHT channels are given minimum distribution and receive the security protection their contents warrant.

9. Working papers and similar documents containing information of the types listed in Annexes A and B need not, at the discretion of the officer in charge and after full consideration of the risks involved, bear the classification, codeword or handling caveat when handled exclusively within a COINHT secure area by indoctrinated persons.

- 2 -
CLASSIFICATION

10. The classification of each document containing information related to COMINT or CHINT activities must be determined individually, after due consideration of the damage which unauthorized disclosure of its contents could cause to national security, national interests, and the capability of either party to continue to produce communications intelligence.

PUBLIC STATEMENTS

11. Maximum feasible administrative action will be taken to require that all public statements which may contain information related to COMINT or CHINT activities are submitted, for preliminary review and advice, to the appropriate COMINT authority, as specified by either Board. In the event that such information already publicly revealed is included in a document submitted by a private source for review, an attempt by persuasion shall be made to eliminate such information or to express it in such general terms as to conceal, to the maximum degree possible, specific associations with COMINT activities. In the event such a document is submitted by an official source, that document will be classified in accordance with paragraph 10 above.
TYPES OF INFORMATION TO BE GIVEN THE SAME PROTECTION AS COMINT

1. When information which is neither COMINT nor that contained in the "documents and technical material" referred to in paragraph 19 of Appendix B, indicates:
   (a) a degree of success or progress being made in the production of communications intelligence, or
   (b) a sophisticated COMINT technique, or
   (c) the scale and direction of the COMINT effort to a degree which may stimulate countermeasures,

it must be accorded the protection of the classification and COMINT codeword appropriate to the highest category of COMINT to which it relates, and will be kept within COMINT channels unless released therefrom by proper authority designated by USD or DCS. If the category of COMINT to which the information relates is not known, it will be accorded the protection of the highest category.

2. Examples of the kind of information which may reveal (a), (b) or (c) above are:
   (a) Consumer requirements for information from a specific source.
   (b) Detailed characteristics and capabilities of equipment as applied in the exploitation of COMINT.
   (c) Details of COMINT-developed techniques used in COMINT research or production.
APPENDIX B

ANNEX XI

ANNEX XI

TYPES OF INFORMATION TO BE HANDLED VIA COMINT CHANNELS ONLY

1. Information which does not require codeword protection but which relates to COMINT or OOKINT activities will bear the classification indicated (but no codeword), will carry the caveat "HANDLE VIA COMINT CHANNELS ONLY" and be retained in COMINT channels unless exempted or released in accordance with procedures established by USIS or DCS.

TOP SECRET

2. Information relating to COMINT or OOKINT activities will be classified TOP SECRET if the unauthorized disclosure of it could result in exceptionally grave damage to national security, national interests or the continued conduct of COMINT operations. Examples of the kind of information which may warrant this classification are:-

   (a) A plan, doctrine or policy or information on tasking or control which reveals specific COMINT operations of major importance.

   (b) A plan, doctrine or policy or information on tasking or control which reveals specific COMINT operations of major importance.

   (c) A plan, doctrine or policy or information on tasking or control which reveals specific COMINT operations of major importance.

   (d) A plan, doctrine or policy or information on tasking or control which reveals specific COMINT operations of major importance.

SECRET

3. Information relating to COMINT or OOKINT activities will be classified SECRET if the unauthorized disclosure of it could result in serious damage to national security, national interests or the continued conduct of COMINT operations. Examples of the kind of information which may warrant this classification are:-
(a) A plan, doctrine, or policy or information on tasking or control which reveals important specific CONINT operations.

(b) Base rights negotiations for CONINT sites, which involves disclosure of the specific purposes for which the sites are intended.

(c) Important construction and budgetary information relating to CONINT collection and processing organizations and installations.

(d) Individual intercept assignments.

(e) Detailed D/IV plans and overall operational effectiveness of D/IV organizations.

(f) All personnel reports and documents, civilian and/or military which indicate authorized and/or actual agency CONINT strength in total, by job designation or by organizational element title where such designation or organizational element title would indicate details of the CONINT mission.

CONFIDENTIAL

1. Information relating to CONINT or OXINT activities will be classified CONFIDENTIAL if the unauthorized disclosure of it could be prejudicial to national security, national interests or the continued conduct of CONINT operations. Examples of the kind of information which may warrant this classification are:

(a) A plan, doctrine, or policy or information on tasking or control which reveals specific CONINT operations of a minor nature.

(b) CONINT indoctrination and debriefing statements.

(c) Lists of CONINT indoctrinated and debriefed personnel.

(d) Information which reveals extent of effort or special purpose features of electronic computers as utilized for CONINT processing, without revealing CONINT techniques.

- 6 -

TOP SECRET DAUNT
APPENDIX B

ANNEX C

TYPES OF INFORMATION WHICH MAY BE HANDLED IN ACCORDANCE WITH NORMAL SECURITY REGULATIONS

1. Information pertaining to COMINT which neither requires code word protection nor the caveat "HANDLE VIA COMINT CHANNELS ONLY" will be classified and handled in accordance with U. S. or Canadian governmental security regulations in effect for information unconnected with COMINT or COMINT activities.

SECRET

2. Information, the unauthorized disclosure of which could result in serious damage to national security or national interests, will be classified SECRET.

Examples of the kind of information which may warrant this classification are:

(a) Construction and budgetary matters pertaining to COMINT collection or processing organizations and installations, provided no reference is made to their specific functions.

(b) Base rights negotiations for COMINT sites, provided no mention is made of actual purposes for which the sites are intended.

CONFIDENTIAL

3. Information, the unauthorized disclosure of which could be prejudicial to national security or national interests, will be classified CONFIDENTIAL.

Examples of the kind of information which may warrant this classification are:

(a) Personnel reports and documents, civilian or military, which indicate authorized or actual COMINT agency strength in total, by organizational element, short title or symbol, by primary element, or by function.

(b) Regulations stating the general mission and functions of COMINT activities that do not reveal specific COMINT techniques or procedures.

(c) Correspondence on hazardous duty restrictions pertaining to individuals released from COMINT assignments.

UNCLASSIFIED

4. Examples of the kind of information which is UNCLASSIFIED are as follows:

- 7 -
(a) Cover names assigned to "Rapid Analytic Machinery" (RAM) when used out of context.

(b) The terms "Communications Intelligence" and "COINTE", "Signals Intelligence" and "SIGINT" when used out of context.

(c) References in broad, general, non-specific terms to intercept, direction finding, voice operator analysis and radio fingerprinting as sources of intelligence.

(d) Elementary principles of traffic analysis, military cryptanalysis and cryptography.

(e) Mention of interest in computer type circuits, if no indication is made to type of systems in which they are to be used.

(f) Individual job titles and descriptions that do not contain information otherwise listed above as requiring classification.

(g) Project numbers and titles used in justification of purchase of materials when no technical usage is specified.

(h) The fact of association between any U.S. or Canadian COINTE agency providing it is not shown to be in the COINTE field.
APPENDIX C

EMERGENCY PLANNING

1. The word "Hostilities", whenever used in this Appendix or Annexures thereto, is defined as a state of war or a similar situation in which both the United States and Canada are actively involved.

2. Both parties agree to the necessity for combined COMINT emergency plans to be placed into effect at, or before, the outbreak of hostilities. It is understood that such plans are liable to modification in whole or in part by governmental or staff agreements or decisions made at a higher level.

3. It is agreed that a threat of hostilities, or developments after hostilities begin, may necessitate:

(b)(1)
(b)(3) - 18 USC 798(a)
ANNEXURE E
To
APPENDIX C

(b) (1)
(b) (3) - 18 USC 798(a)
### APPENDIX E

**TABLE A**

<table>
<thead>
<tr>
<th>Column 1</th>
<th>Column 2</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**EXHIBIT 1**

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

---

**TOP SECRET COPY**
### Table B (Cont'd.)

#### APPENDIX E

#### EXHIBIT 1

(b)(1)
(b)(3) - 18 USC 798(a)
(b)(3) - 50 USC 3024(l)
(b)(3) - P.L. 86-36
APPENDIX E
EXHIBIT 2

(b) (1)
(b) (3) - 18 USC 798(a)
(b) (3) - 50 USC 3024(1)
(b) (3) - P.L. 86-36
(b) (1)
(b) (3) - 18 USC 798(a)
(b) (3) - 50 USC 3024(j)
(b) (3) - P.L. 86-36
(b) (1)
(b) (3) - 18 USC 798 (a)
(b) (3) - 50 USC 3024 (d)
(b) (3) - P.L. 86-36
APPENDIX E

EXHIBIT 3

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

COORDINATION IN TRANSLATION, AND EXCHANGE OF PERTINENT MATERIALS AND INFORMATION

1. Translated texts, extracts, gists, (unless excepted by para. 5 below), items of Traffic Intelligence, COMINT GADS, and comments appended thereto, will be exchanged upon the specific request of each party, or when determined by the producing party to be of interest to the other. This exchange normally will be effected through the regular liaison channels, although such exchange may be effected by electrical communications when specifically requested by either party.

2. If either party considers the decrypts or plain texts serve its intelligence needs without translation, such decrypts or plain texts will be regarded by the other as if they were translated texts and their exchange between the parties will be precisely the same as that of translated texts and extracts (see para. 1 above). It is the intention of each party to limit such cases to the minimum.

3. Decrypts will not be exchanged between the two parties, except as above, or as may be arranged for cryptanalytic or other technical reasons. Any decrypts or series of decrypts will be made available on specific request by one party to the other, if not prohibitively inconvenient.

4. Inasmuch as the parties to this Agreement will probably be unable to translate all decrypts or plain texts in full or even in part, each will carry out a process of scanning such as will meet its own requirements. The liaison officers will be free to modify this material to ensure that any particular interests of their own party are being served.

5. Gists which are made by a party for its own use but not issued will not be exchanged but will be at the disposal of the liaison officers as may be required.

6. CSB and APMA will constitute the channel through which all Communication Intelligence items produced by Agencies of one party will be forwarded to Agencies of the other. Any exceptions to the foregoing will be made only with the specific approval of both CSB and APMA in each case.

STANDARDIZATION OF TRANSLATION FORM

7. To avoid ambiguity and to promote ease of handling, reference, and recording, it will be the aim of the Canadian and U.S. Agencies to adopt a standard style and layout for headings, translated texts, gists, extracts, comments, and translators' notes.

STANDARDIZATION OF TRANSLATION CONTENT

8. Each Agency will furnish to the other upon specific request, copies of Supplementary Glosesaries and other compilations which it prepares as a result of and for use in its translation processes. The materials thus exchanged will be the basis for con-
APPENDIX V

Continuous discussion between the Agencies with a view to increasing standardization.

9. In order to develop a common standard of validity grading in language equivalents, each Agency will inform the other of the significance of such gradings as it currently uses in its Supplemental Glossaries.

10. Translated texts will be assumed to be in full unless labelled "gist" or "extract".

11. Comments will be clearly distinguishable as such and will be prefaced by the word "Comment".
APPENDIX C
COMBINED COMMUNICATIONS

1. COMMUNICATIONS ORGANIZATION

(b) (1).
(b) (3) - 18 USC 798(a)
(b) (3) - 50 USC 3024(l)
(b) (3) - P.L. 86-36
APPENDIX B (1)
to
APPENDIX C

COMMUNICATIONS FOR DE-LOCATED ACTIVITIES

(b) (1)
(b) (3) - 18 USC 798 (a)
(b) (3) - 50 USC 3024 (1)
(b) (3) - P.L. 86-36
ANNEXURE B (2)
TO
APPENDIX C

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

April, 1951

TOP SECRET
ANNEXURE B (1)
to
APPENDIX C
COMMUNICATIONS FOR IN-LODED ACTIVITIES

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

April 1, 1951

TOP SECRET
ANNEXURE B (4) TO
APPENDIX C

- TOP SECRET -

COMMUNICATIONS FOR RE-LOCATED ACTIVITIES

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

April, 1951

TOP SECRET
APPENDIX I

EXCHANGE OF RAW TRAFFIC

AND STANDARDIZATION OF RAW MATERIAL FORMAT

EXCHANGE OF RAW MATERIAL

1. Each party will furnish to the other, as promptly as practicable without request and as a matter of routine, one copy of every item of raw traffic collected by its operating agencies which is of a type required by the other party. Either party may request expedited delivery, or additional copies, or specific categories of raw traffic and each shall endeavor to meet the needs of the other in this respect.

2. Impractical or practically incapable raw traffic exchanged will be in the forms indicated in paragraphs 4 - 8 below.

3. The inclusion of a case-number in an item of raw traffic is not deemed to allow evidence of processing for Communication Intelligence purposes and therefore the material may still be classified CONFIDENTIAL.

STANDARDIZATION OF RAW TRAFFIC FORMAT

---

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

---

TOP SECRET COPSE
(b) (1)
(b) (3) - P.L. 86-36