

~~TOP SECRET~~

R23



NATIONAL SECURITY AGENCY  
FORT GEORGE G. MEADE, MARYLAND

# CRYPTOLOG

JANUARY 1975



EO 1.4.(c)

P.L. 86-36

UNNA, [redacted] .....	[redacted] .....	1
THE SIGINT USERS' HANDBOOK.....	Donald B. Oliver.....	3
HOW CLEAN DOES A DATA BASE NEED TO BE?...	[redacted] .....	5
THE YAWN OF THE COMPUTER AGE.....	[redacted] .....	6
THE CASE FOR COMINT READERS.....	[redacted] .....	7
CROSSED CODEWORDS.....	[redacted] .....	9
CLA IS TEN YEARS OLD.....	[redacted] .....	10
OTHER NEWS FROM THE LEARNED ORGANIZATIONS.....	[redacted] .....	12
INDEX OF CONTRIBUTORS FOR 1974.....	[redacted] .....	13

~~Classified by DIR/NSA/CICSS (NSA/CSSM 123-2)  
Exempt from GDS, EO 11652, Category 2  
Declassify Upon Notification by the Originator~~

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~TOP SECRET~~

# CRYPTOLOG

Published Monthly by P1, Techniques and Standards,  
for the Personnel of Operations

VOL. II NO. 1

JANUARY 1975

PUBLISHER

WILLIAM LUTWINIAK

BOARD OF EDITORS

Editor in Chief ..... Doris Miller (5642s)  
Collection..... [redacted] (3571s)  
Cryptanalysis..... [redacted] (8025s)  
Language..... [redacted] (5236s)  
Machine Support..... [redacted] (3321s)  
Special Research..... Vera R. Filby (7119s)  
Traffic Analysis..... William J. Jackson, Jr. (3369s)  
Art Editor..... [redacted]

P.L. 86-36

\* \* \* \* \*

Editor for December ..... [redacted]

~~TOP SECRET~~

~~SECRET SPOKE~~

# UNNA

by

P.L. 86-36

In his article [redacted] in the September '74 issue of CRYPTOLOG, Derek Craig succinctly stated a pressing problem.

According to the gloomy prognostications of certain writers, the British banking system is already balanced precariously on deposits of Arab wealth which can be redeemed at any moment. The daily newspapers report that Arab efforts to acquire Lockheed Aircraft Corporation have been forestalled. Rumors of an impending purchase of IBM by Arab interests are denied. Arab wealth has already begun to insinuate itself into the fabric of Western economies at some very sensitive spots.

The situation bears watching. The economies of Britain and the United States, foundering under the forces of shortages, recession, inflation, and domestic despair, are vulnerable to disruption, and the Arabs seem not averse to creating mischief.

"It is critical," says Mr. Craig, "for United States policy makers to know how [redacted]"

[redacted]

[redacted]

UNNA\*

[redacted]

[redacted]

*\*Ed. note: This is not an acronym, as you might suppose, but an R task covername. The pronunciation most often heard here is "Oona."*

[redacted]

All the AP requires is a properly ordered directory.

In addition to the "search" function, the AP can, under computer control, do the following:

- Add an entry to core, in proper order;
- Delete an entry from core, and adjust remaining entries;
- Read an entry from a designated core address;
- Write a word into a designated core address;
- Clear core (put all 1's into all of core).

UNNA was designed and developed in R33, with C65 contributing to software development. The device underwent engineering tests [redacted]

[redacted]

~~SECRET SPOKE~~

~~SECRET SPOKE~~

UNNA, as now configured, collects data on magnetic tape.

[redacted] The TAP inputs from the TCD 25 pairs of signal for each voice channel. One signal constitutes parts of 25 different data bit streams (the telegraphy channels) and the other consists of an "energy bit" per channel. Each bit of the data

UNNA Functional Description

UNNA is divisible into four parts: Time Compression Demodulator, [redacted]

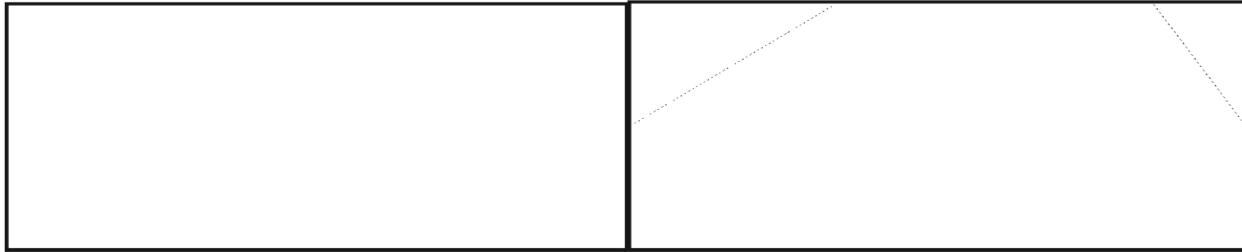
[redacted] Associative Processor (already described), and Honeywell DDP-516 Computer with peripherals.

Time Compression Demodulator (TCD). [redacted]

Computer (DDP-516). The computer used in the UNNA system is the Honeywell DDP-516, with 32K memory. In the "stand-alone" mode it has the following peripherals:

- mag tap controller and two mag tape units, device speed: 36 ips, 556 or 800 bpi,
- card reader and reader control unit, device speed: 200 cpm,
- data terminal (typewriter), device speed: 10 cps, 75 characters per line.

~~SECRET SPOKE~~

~~SECRET SPOKE~~~~(SECRET SPOKE)~~

# the SIGINT USERS' HANDBOOK or: what's an Ishtar?

donald b. oliver, v2

Few NSA employees are aware that since April 1974 a growing body of SIGINT-related information has been appearing under the title SIGINT Users' Handbook. Inasmuch as it is distributed narrowly in-house, even within the DDO organization, and is essentially "uncoordinated," few analysts know that it exists. This should not be surprising, however, as the Handbook's title advises that it is intended for the delectation of SIGINT *users* (also known as consumers or customers) rather than SIGINT producers.

There have been two relatively similar predecessors to the Handbook--a long-lived series titled the "INFOCON" (Information for Consumers) and another series called "Notice to Users" (the latter being an interim step between the INFOCON and the present Handbook). Like the MUSSO system and certain other current vehicles of NSA direction, the INFOCON program suffered from lack of staff attention, lack of interest on the part of NSA managers, and a degree of executive resistance to the whole idea. For whatever reasons, INFOCONS became tired, out-of-date, and of little value to those they were intended to serve. Only the users of SIGINT and those most intimately involved with them, NSA field elements, tried--unsuccessfully--to breathe life into the moribund body.

With the development of a system of United States Signals Intelligence Directives (USSID) which changed, and reflected changes in, the ways we supported the outside world, it was obvious to the SIGINT Directives element (now V13) that the INFOCONS should be reissued or wiped out.

A home for them was hard to find. The old P2 organization, which included a "customer relations" function, felt that P1 ought to do something. P1 allowed as how the effort was "educational," and the National Cryptologic

School should pick it up. The School was unimpressed with that argument. P2 finally got the job, but couldn't come to grips with the major policy issue as to whether an entire package must be presented to the users or whether the job could be done piecemeal. Because of this, little was done.

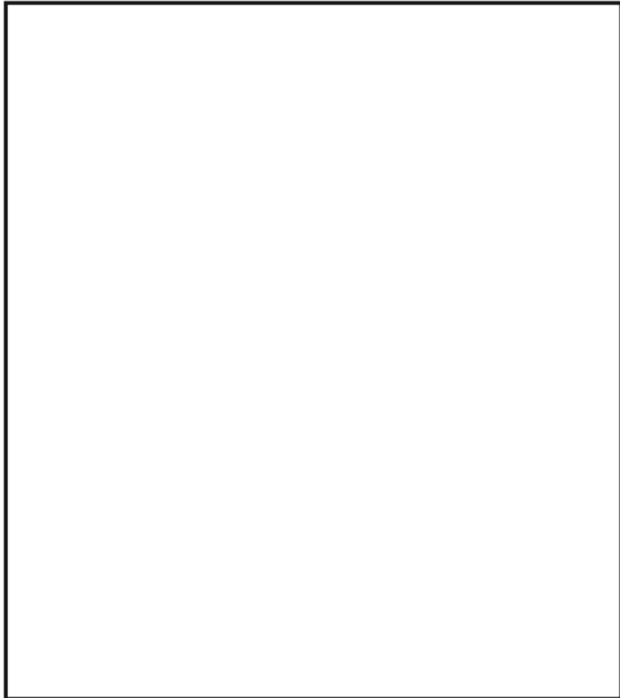
To be fair, however (as I can be occasionally), there was some executive resistance to perpetuating a body of SIGINT information in a formal, structured sense for the education of readers of product or the beneficiaries of SIGINT support. This view was based on the entirely reasonable position that the more users knew of "SIGINT Production Information" (see USSID 300), the more likely they would be to act to take over the responsibility of DIRNSA to manage the SIGINT activities of the United States. It was the view of some executives that little information about SIGINT need be in the hands of the users, and that what was needed could be handled by ad hoc memoranda, letters, and messages.

As is normal, of course, and as soon as it was convenient and safe, this policy guidance was ignored, and the SIGINT Users' Handbook was developed by V2 (now V12).

To a large extent the rationale for the Handbook is the same as for Cryptologic Support Groups. Each has a task of "interpreting SIGINT," advising the user how and in what form product and other SIGINT support can be made available to him, and, in a generally nontechnical context, explaining to him the methodologies, procedures, conventions and systems by which SIGINT is produced and distributed. Particularly within the military community, it has long been true that intelligence assignments are short, and the opportunity and inclination to study and understand the arcane ways of the US SIGINT System are limited.

~~SECRET SPOKE~~

~~CONFIDENTIAL~~



courageous and feisty since it competes (successfully) with DoD Manual 5200.17 (M2) and CIA's Communications Intelligence Security Regulation in this regard. [redacted] of V12, the Handbook scribe, is fearless and overcomes all obstacles.

The Handbook has become a "best seller" in the user community. DIA conducted a survey of DoD SIGINT users last summer and observed:

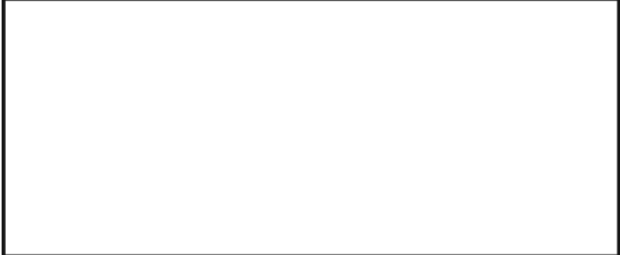
"The SIGINT Users' Handbook is a very valuable guide for all SIGINT users, particularly intelligence analytical personnel. Experienced analysts find the Handbook a very useful reference document; it is invaluable to the new or inexperienced analyst as an information guide and tool relevant to SIGINT operations. In this vein, it can be used for indoctrinating new personnel relative to the various SIGINT reporting vehicles, retrieval systems, general composition of SIGINT product and concepts of SIGINT support and operations. The Handbook can be viewed as the SIGINT 'primer,' and for the new or unindoctrinated, supplements knowledge of SIGINT acquired through the NSA orientation/familiarization courses."

EO 1.4.(c)  
P.L. 86-36

A word of caution. Although geared to the USSIDs, the Handbook is not a suitable replacement for those documents in respect to SIGINT producers. Nor should it be used as a reference work to pass tests.

If you would like to review the Handbook, or if you have subjects which you believe are candidates for inclusion therein, I suggest that you call or visit [redacted] (ext. 5283s).

P.L. 86-36 ~~(CONFIDENTIAL/HVCCO)~~



# OPPORTUNITIES

PROGRAMMERS AND BOOKBREAKERS PLEASE NOTE: The "Checklist for Programmers of Machine Support Tools for Bookbreaking" by Katharine Swift and [redacted] (8 pages) is now available. Copies can be obtained from [redacted] P16, 3W070, ext. 3045s.

LEARNING CENTER OPEN IN NEW LOCATION. The Learning Center in OPS 1 has been relocated to Room 2W165 and its capacity more than doubled. Hours are 0700 to 2100, Monday through Friday. Self-paced courses are available in effective reading, writing, speaking and listening; basic

digital computer theory, electronic data processing, computer systems performance, slide rule operation; refresher courses in algebra and transistors; courses in English as a second language and women in management.



HELP WANTED. Among a number of things in which the National Security Agency is interested is ELINT. Yet CRYPTOLOG has never had a word about it, except perhaps in passing. I will accept part of the blame for that, as I just do not know enough about the subject. There is a vast number of people, however, even in CRYPTOLOG's readership, who do know enough about the subject to educate the rest of us. Please let me have something on this subject. Collection Editor.

~~(CONFIDENTIAL/HVCCO)~~

EO 1.4.(c)

~~CONFIDENTIAL~~ HANDLE VIA COMINT CHANNELS ONLY

~~CONFIDENTIAL~~

# HOW CLEAN DOES A DATA BASE NEED TO BE ?

P.L. 86-36

by [redacted]

One of the first things one learns about computers is that they require a much higher order of accuracy in the material they manipulate than do comparable "human" processes. One learns to pay an extra measure of tribute in the form of added proofreading or other forms of quality control, so that the input is "clean" enough for the computer to handle.

After a while, as the novelty wears off, it sometimes occurs to one that not all of the data needs to be so awfully clean. If we expect to sort or retrieve on a particular field or data element, then that field or data element should be clean and garble-free; but if a neighboring item is never (well--almost never) used as a control for sorting and retrieving, then it only needs to be as garble-free as people need. Quite clearly, if only half of your data elements really need quality control, then some of that manpower now spent scrubbing each little data element might be diverted to other tasks.

It is possible to imagine categorizing data elements as "first order" if they need to be "computer clean," and as "second order" if they only need to be "people clean."

In this day of great monolithic data bases, however, the use of varying quality levels can cause troubles, however laudable their manpower savings may be. A story "from life" will illustrate

Some years ago, during the Vietnam War, we found ourselves receiving two streams of electrical material from the sites in the field, and both streams were used to feed computer processes

[redacted]

The second was a cryptanalytic stream. A

[redacted]

The specific details of these processes belong to another story (or series of stories). The point here is that there came a time when there was an operational need to identify which messages

[redacted] It should have been easy. Neither system was new, and both had been working for quite a while with reasonable success. (Success is a relative term; there were always problems, sometimes earth-shaking problems, but by and large, the systems did work.)

[redacted]

It took a while to find out why, but after a time the answer became clear. Evidently the people at the sites, knowingly or unknowingly, practiced different levels of quality control on the various data elements.

[redacted]

All of which suggests several thoughts.

Garble rates can often be determined, at least approximately, by machine. Certainly differential garble rates can be (Field 1 has more or fewer garbles per thousand than Field 2). If data bases which now exist were measured to show which data elements were "cleanest" and which were "dirtiest" (perhaps arrayed in a sort of quality hierarchy),

EO 1.4.(c)  
P.L. 86-36

- ◆ the unwary might be warned off using the data base for sorting or controlling on the wrong (dirtiest) data elements;
  - ◆ hit thresholds might have to be lowered when dealing with "dirty" elements, even at the expense of wading through more "garbage" output;
  - ◆ managers might better understand the manpower costs of various control strategies;
- but also:
- ◆ we might decide that great monolithic data bases are not always the answer when one must work with a variety of data sources having widely different notions of which items are "important."

~~(CONFIDENTIAL/HVCCO)~~

~~CONFIDENTIAL~~ HANDLE VIA COMINT CHANNELS ONLY

# THE YAWN OF THE COMPUTER AGE



OR  
When Your Terminal Is Terminal....

by   N22

P.L. 86-36



It's no secret that NSA has become almost totally dependent on computer systems to aid our analysts. The fact is, we have had to turn to these systems in order to handle the increasing volume of work, that grows more sophisticated while our peoplepower is shrinking. But this dependence on computer systems has not been without its drawbacks and frustrations. I'd like to call your attention to one of these.

It's bad enough that the (expletive deleted) computers are down several times a day, but that's something we have been conditioned to expect. The real crime being perpetrated on systems users in NSA is far more difficult to adapt to. It is the dreadful excuse given in accompaniment of each system failure or blowup.

"Power problem on the platform," some anonymous voice monotonizes to you over the phone. Or worse still, "Don't know. The --- Representative's looking at it now." I ask you, where's the satisfaction in explanations like these?! We users are looking for a salve, and instead we receive the same infuriating excuses time after time.

Well, I have a suggestion (worked out while awaiting the reactivation of a lifeless terminal). Let's have a contest. Users will send in their nominations for reasons to explain the systems failures. The best of these will be selected for play on taped telephone messages. Naturally these will have to be changed several times a day, coinciding with the actual systems failures. We could even institute a method whereby after the message ended the caller would have 20 seconds of the tape to vent his frustrations as a system user. This suggestion could pay for itself because NSA would then accumulate all these 20-second rages into 18½-minute segments and sell them to GSA, who would play them on tape decks hidden in statues, to keep pigeons at a respectful distance. Or better yet--what NSA walker hasn't wished for a way to prevent birds from "roosting" (you've got another name for it?) along the covered portions of our sidewalks? Cleaning bills alone could offset the expense of this suggested application.

Now, just to show you what I have in mind as the type of excuse that users are looking for, here are several examples:

1. In accordance with provisions of the Fair Labor Standards, the computer is at lunch.



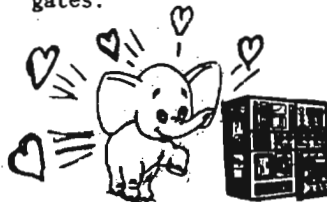
2. When we fed all NSA's Regs and Procedures into core, the computer blew up.

3. Unfortunately the GSA standby crew just stood by.

4. An enraged bull gored the CPU and all the electrons leaked out.

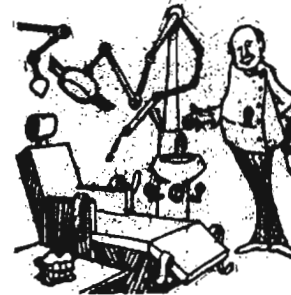


5. The main frame's been recalled by the manufacturer. There's some problem with the MAYBE gates.



6. An amorous elephant tried to mate with the CPU. We expect a doubling of processing capability in about two years.

7. The orthodontist is here now, trying to correct the computer's overbyte.



Sure, I realize that this suggestion isn't going to keep our systems up any more of the time than they are up now. But at least users can be provided with a slight diversion from this irksome and perplexing problem. Maybe, too, the competition to get an excuse accepted will increase systems utilization, reduce sick leave, and improve morale. (That last "e" was changed from "s" by the censor.) We would require hundreds of excuses per week, so conceivably everyone in the Agency could eventually win.

Anyway, what could it cost NSA to offer a token prize for an accepted excuse? I think our people would be satisfied with a hammer, a chisel, and a slab of rock. Then they could create their own data files.





~~TOP SECRET UMBRA~~

# THE CASE FOR COMINT READERS

by [redacted] P16

P.L. 86-36

The following article (with some footnotes which have been omitted here) originally appeared in QRL in May 1971. For other views on this subject see the June 1971 Keyword and the August 1971 QRL.

**At** the time of this writing, I have participated in the preparation and grading of four Spanish-language Professionalization Qualification Examinations and have seen more than half of the examinees flunk one or more parts. A few people have expressed the opinion that the high failure rate stems from the fact that the test was too hard. Depending on how you choose to define the expression "too hard," they may be right.

The committee charged with making the exam and grading it started from the assumption that being a qualified Spanish linguist at NSA is a hard job. A true "professional" should be able to handle any kind of Spanish material that comes at him--from any country, on any reasonable topic, [redacted] in good condition or corrupt, written or spoken, etc., etc. Perhaps any test that tried to prove a person's capabilities in all those respects might be called "too hard," but the ability to handle those topics and types of traffic differentiates an NSA linguist from other linguists.. and there are people who can deal with those various problems; this fact can be attested by the large number of people who have managed to pass the PQE despite its difficulty.

With Spanish, the problem is complicated by the number of countries using the language (most of which have some particularly irksome national usage--telegraphic abridgement, vocabulary, abbreviations, etc.).

[redacted]

[redacted]

As lovely as it sounds, it is totally impractical because it would actually slow down production while old-timers--assuming that they hadn't been transferred to another section to learn something else--took time from their work to explain things to the "new boy"; supervisors would be justifiably reluctant to transfer qualified linguists out to pick up new skills while getting a bunch of unskilled people to teach; even the linguists involved would object to spending time to learn something and just when they're gaining proficiency in it they'll have to leave it and go learn something else; in addition, the constant shifting and acquisition of new bosses might hinder their chances for promotion.

All of these disadvantages seem to outweigh the advantage of having a corps of well-versed linguists. I think it goes without saying that such a nucleus of all-around linguists is certainly a good thing to have, but it just isn't a good thing to go to all the trouble of getting one.

Another possible method of familiarizing linguists with all the sorts of problems they're likely to encounter in a given language is to have a division or group training office which prepares a broad course to teach the requisite subjects, using material from a number of sources.

[redacted] Naturally, this material would be arranged in order of difficulty, starting out with easy and uncorrupt text and advancing into more telegraphic styles, first without and then with garbles.

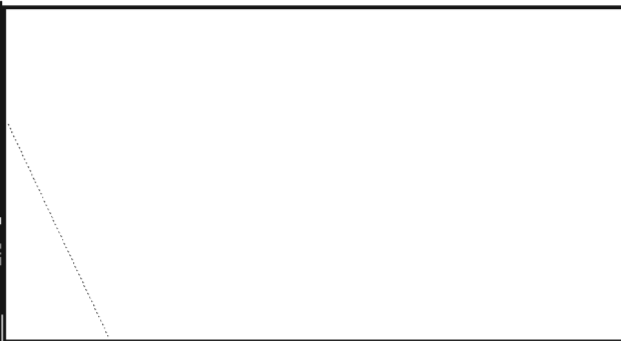
EO 1.4.(c)

Problems involved in having such a course include: whether or not it actually includes all the types of material required; whether the amount of time allotted to the various topics is adequate; whether all the people who should take it do so (or are allowed to by supervisors who hate to take people away from production, even for a course which might improve output); whether taking such a course should be a prerequisite for taking a PQE; whether the grading is too strict or too lenient; whether the course content is changed and updated from time to time; and the obvious question: How many people who take the course subsequently go on to pass all parts of a Professionalization Qualification Examination? (This may seem like an "obvious" question, but it's hardly a fair one, since that isn't really what such a course should be designed for; however, one might be tempted to consider the PQE as a way of verifying the effectiveness of the course).

P.L. 86-36

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~



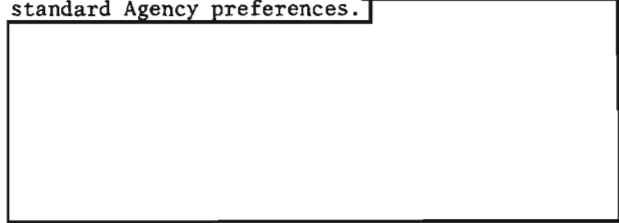
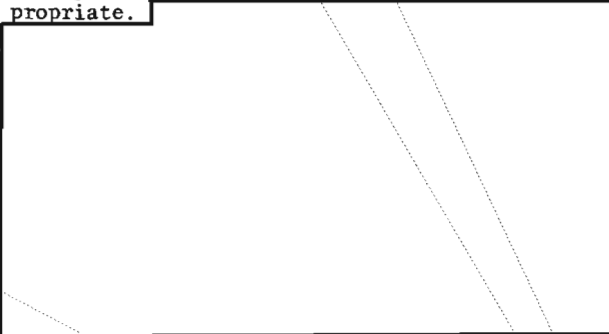
Here a word of caution should be given. There ought to be a reminder of acceptable degarbling procedures, and garbled groups should be restricted to one wrong letter (or digit) or one pair of transposed characters per group. Obviously, the code groups must be shown to enable the user of the COMINT Reader to degarble mutilated groups. The groups that are garbled should, if possible, appear elsewhere in the text to help the degarbling process.

Perhaps a brief outline of what a COMINT Reader might include would be helpful. After introducing texts on a number of subjects, duly notated to show telegraphic usage



garbles can be introduced: wrong letters, missing letters, transposed letters. These mutations should be explained, preferably in a special "Answers" section, either at the back of the book or in a separate volume, and sample translations given. This latter feature would introduce the user to standard Agency preferences.

A variation of this practice might be introduced in the one-part code section where the message text obviously calls for a word with a given meaning and the alphabetical range of the code pins down which of several synonyms is appropriate.



was to help individuals pass PQE's (although I sincerely hope that no one feels that this is the only value of COMINT Readers), it should be remembered that such garbles have no place in professionalization exams.

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

The final printout [redacted] should be accompanied by a wealth of explanatory notes, as well as an acceptable translation. (Apropos of "an acceptable translation," it doesn't take long until it becomes "the acceptable translation" and perhaps there should be a few paragraphs explaining why certain choices are unacceptable; [redacted])

The COMINT Reader has one advantage over a regular course; namely, that the student can progress at his own rate of speed, rather than try to keep up with a class (which may mean going on to a new topic before he really understands the old one). In addition, the user can keep the book in his desk, studying it only when his workload permits (although if supervisors will let their people spend one or two hours per day working with the COMINT Reader, that would be commendable).

The availability of a COMINT Reader does not necessarily obviate having a formal course; the two can complement each other. In fact, the use of a CR as a text for such a course is quite a possibility, and a knowledgeable teacher could clarify the explanations and comments that the original compiler may have treated too briefly. A teacher can also acquire additional material to reinforce the lessons in the Reader, or to give specific individuals greater practice in handling the types of traffic with which they are actually working. A current piece of traffic may provide a better example of some phenomenon than the message shown in the COMINT Reader. (In other words, just because such a book has been published, this doesn't mean that the canon has been closed once and for all.) In fact, this is one advantage that a class can have over a CR.

Naturally I don't propose COMINT Readers for every language. In some cases, the traffic does not offer the variety of users that the common languages [redacted]

[redacted] provide. There are some languages where the volume is so small that one or two linguists get a chance to handle all the different types; there are other languages where the number of potential Agency employees who could profitably use a CR is so small that the time and effort spent in producing one could not be justified. But I do feel that such books would be valuable to NSA in helping people pass PQE's and--more important--to give Agency linguists a better understanding of some aspects of their language so that they can do a better job.

There are still a number of questions about COMINT Readers left unanswered. For example, who will prepare them? How can we be sure that all available type of material are included? How can we be sure that the material is correct?

Will they really work? There may be other questions, but these four should hold us for a while.

P.L. 86-36  
EO 1.4.(c)

A COMINT Reader should not be a one-man show or solo operation, especially for those languages where the input will come from a number of Agency components. To be sure, one person could be the committee chairman or editor-in-chief, but there should be several checkers, training officers, and other qualified linguists responsible for the selection, arrangement, translating and explicating.

P.L. 86-36  
EO 1.4.(c)

The obvious way to make sure that the material is comprehensive and correct is to have the greatest possible number of Agency elements using the language represented in that preparatory committee, and to staff it only with qualified linguists of recognized ability. Naturally they will have access to a broad range of materials classified up to and including TOP SECRET CODEWORD, which will most likely be the classification of the COMINT Reader. Having a sufficiently high security classification will also allow for a fairly complete inclusion of all sorts of appropriate material.

As for the last question, about whether COMINT Readers will really work, I honestly can't say. But I firmly believe that since the rotation system is impractical, and the setting up and holding of classes is a more complicated procedure (and has its drawbacks), COMINT Readers certainly ought to be given a chance. We won't know until we've tried--and, assuming that the CR idea will work, we ought to try it soon!

~~(TOP SECRET UMBRA)~~

CROSSED CODEWORDS  
19 UKUSA COMINT CATEGORY DESIGNATORS  
USED OVER THE PAST 24 YEARS  
by [redacted]

P.L. 86-36

ACTIOSUZSUMORAYTOVIP  
MMXSHSTATTEMECTLZOU  
BMBTOATISETHC AKETT  
ILSLKBERDVTECCOMFART  
OYKMERREMAAEEETAPLAI  
UDAXYEDRAMLLAMNRSRNL  
SAEONEOEQUINTRUNTR  
ZZROUTELFIRUALSOEVEN  
OEESTLLODAUNTDTBHAMES  
ODNEXERXALAXEMBSEVAE  
MONEYVLAYNDIEMERRZY  
YSAVINLELLKGD IRBMT  
MAINCANOEOAANMLOSUF  
RIGXIOUMENUNTMOOR  
ALCMUSLETIETIATOKLSAR  
MENUMPPSRDDAU YBESOKS  
SDROEOZEEIEOTYZOONS  
IQKSAOENRXNETZBOFXIA  
DENARKETEDLAARB MUUSL  
NILLIKROYWENRAINROFI

EO 1.4.(c)  
P.L. 86-36

~~(SECRET//HVC0)~~

~~TOP SECRET UMBRA~~

~~CONFIDENTIAL~~

January 1975 marks the tenth anniversary of the founding of the Crypto-Linguistic Association. CLA brings together linguists and other professionals of varying backgrounds and interests--the young technician eager to expand his horizons, the veteran seeking to promulgate a theory or present a new technique, the manager anxious to spot new talent or acquaint himself with the latest developments in the field. As a professional and learned society the Association has a duty both to the individual cryptolinguist and to the field as a whole, and in fulfillment of that duty it has steadily expanded its scope and its efforts.

To give cryptolinguists an opportunity to know each other; to acquaint them and other professionals with what is most significant in the field; to provide a forum in which members can present their ideas; to recognize achievements in the field of language at NSA--these are the goals of the Cryptolinguistic Association.

#### Lecture Series

This has been another exceptionally successful year for the lecture series, as attendance has testified. Members and friends have heard Clifford Groce of the Voice of America, Howard Rosenblum, NSA DDR, Brigadier Tiltman of P1, and, as a surprise bonus, Victoria Fromkin of UCLA's Department of Linguistics. The schedule for the next few months is as follows:

Tuesday 14 January	Tenth Anniversary Lecture by Mr. William Hyland, Director of the Bureau of Intelligence and Research of the U.S. Department of State.
Tuesday 11 February	"The Use of a FAST-Trained Linguist in Military Intelligence." Col. Richard A. Szymczyk, Chief of the Western Area Division of the Directorate for Intelligence, Defense Intelligence Agency.
Tuesday 11 March	"Computers and Linguistic Applications," Dr. A. Hood Roberts, Vice President of the Center for Applied Linguistics, Arlington, Va.
Tuesday 25 March	Gala Tenth Anniversary Concert. "Songs from Around the World." The U.S. Army Chorus under the direction of Capt. Allen Crowell.
Tuesday 8 April	"Translation: Science or Art?" Dr. Esther Matteson, Linguistic Consultant with Wycliffe Bible Translators.

(Note: All the speeches presented during the past two years have been recorded on tape, and it is expected that these will be also. The Association is now discussing with the Learning Center the use of its facilities for making the tapes available on cassettes for use within the Agency.)

#### Special Interest Groups

The Association has two special interest groups now active, and two more in the process of formation. All interested members are invited to join one of these groups, or, with the approval of the Board of Governors, to establish a new group in a field of special interest to them.

SIGLEX (the Special Interest Group on Lexicography) was formed in 1972 and has been very active ever since. Some of the subjects in which the group has interested itself are modern methods and standards of lexicography, evaluation of commercially produced dictionaries, review of Agency-produced dictionaries and glossaries, and uses of the plain-language index. Several members attended the International Conference on Lexicography in New York in 1972. President is [redacted] 8407s.

SIGVOICE, as its name implies, is keyed to language in its spoken form, particularly to the work of transcribers and to research which may assist in better processing of voice intercept. So far this season it has taken up the subjects of voice transcription

P.L. 86-36

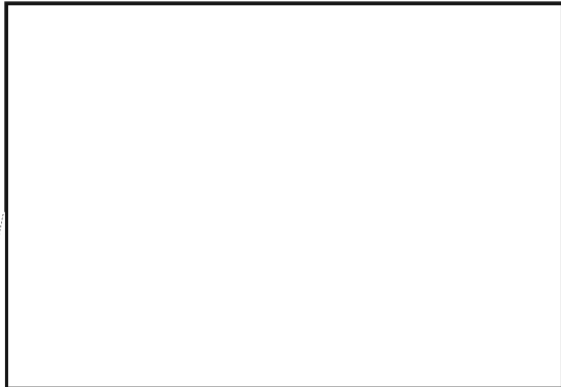
~~CONFIDENTIAL~~ HANDLE VIA COMINT CHANNELS ONLY

~~CONFIDENTIAL~~

EO 1.4.(c)  
P.L. 86-36

at field stations, [redacted] and tactical voice in Vietnam. On 9 January 1975 Dr. Richard Altes of Electromagnetic Systems Laboratories, Sunnyvale, California, will discuss perception in bats, dolphins, and man. In February and March, [redacted] both of R54, will speak on voiceprints and auditory illusions, respectively. Jack Gurin, 5236s, is President of SIGLEX.

A new group now forming is SIGTRAN, which proposes to study the general principles and practices of translation, both inside and outside NSA. "Translation shall be interpreted in the broadest possible sense... [and]... shall closely relate to other fields of cryptologic knowledge, such as cryptography, computer science, and certain other branches of applied linguistics." The first meeting is scheduled for Wednesday, 22 January, at which time Whitney Reed will speak on free-lance translation. Interim chairman of the SIGTRAN group is Florence Kuipers, 4998s.



The Essay Contest

The essay contest is held annually; its purpose is to encourage writing on the application of linguistic knowledge to the solution of Agency problems. Any paper on language, cryptology, or a significantly related subject may be submitted and any NSA employee, regardless of membership in the CLA, is eligible to enter the contest. (Papers which have appeared in any Agency publication during the preceding 12 months will automatically be considered entries.) Prizes of a hundred, fifty, and twenty-five dollars go to the winners. Entries for this year should be submitted in three copies by Friday, 14 March, to [redacted] CLA Secretary, Room 2A197-1.

The Jaffe Award

The Jaffe Award is a memorial to the first president of the CLA, Dr. Sydney Jaffe. It is CLA's highest recognition of exceptional achievement, and takes the form of a citation and the inscription of the winner's name on a plaque on permanent display in the main lobby.

P.L. 86-36

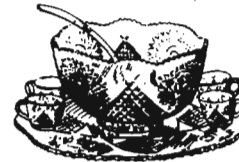
Candidates are nominated for outstanding achievement in one or more of the following:

- Integration of language work with other disciplines
- Linguistic research pertinent to the Agency's work
- Contributions to the effectiveness and morale of linguists
- Management of language operations
- Versatility in working with several languages
- Contributions to language training
- Saving of time and money in language operations
- Contributions involving rare languages
- Development of new equipment, procedures or systems expediting language work
- Scholarly eminence which has made the candidate of unique value as a consultant
- Public achievement which enhances the prestige of the language field.

Individuals may be nominated by any three members of the cryptologic community, by the chairman of the language career panel, or by any supervisor at office level or its equivalent. Nominations should be submitted by 30 March; for details call the CLA President, [redacted] 4332s.

The Spring Banquet

The CLA "season" culminates each year in a banquet in late spring for members and their families and friends. Dinner is preceded by a cocktail hour and followed by a program which typically includes a distinguished speaker on a subject of general interest, the introduction of new officers, and the announcement of the winners of the essay contest and the Jaffe Award.



P.L. 86-36  
EO 1.4.(c)  
EO 1.4.(d)

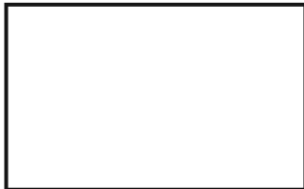
P.L. 86-36

~~CONFIDENTIAL~~ HANDLE VIA COMINT CHANNELS ONLY

# Other News from the Learned Organizations



## NEW OFFICERS



- ✓ PRESIDENT
- ✓ PRESIDENT-ELECT
- ✓ CO3, SECRETARY
- ✓ TREASURER
- ✓ MEMBER-AT-LARGE
- ✓ MEMBER-AT-LARGE
- ✓ MEMBER-AT-LARGE

{\*NEWLY ELECTED}

## 1975 CISI CONFERENCE

THE SECOND CISI SPRING CONFERENCE WILL BE HELD 20-22 MAY 1975 IN THE NSA AUDITORIUM. PAPERS HAVE BEEN SUBMITTED ON FOUR TOPICS:

- SECURITY IN DATA SYSTEMS
- DATA BASE MANAGEMENT SYSTEMS
- FIELD SYSTEMS/APPLICATIONS
- MANAGEMENT IN DATA SYSTEMS

THEY WILL BE PUBLISHED AND DISTRIBUTED TO MEMBERS BEFORE THE CONFERENCE. AUTHORS WILL DISCUSS THEIR PAPERS AT THE MEETINGS.

## LECTURES

THE JANUARY MEETING, TO BE HELD AT 0930 ON 23 JANUARY IN THE NSA AUDITORIUM, WILL BE CO-SPONSORED BY SIG/HUMAN FACTORS. THE SPEAKER WILL BE MAJ. GEN. RIENZI, DIRECTOR OF TELECOMMUNICATIONS AND COMMAND AND CONTROL OF THE DEPARTMENT OF THE ARMY, DISCUSSING "SOME LESSONS LEARNED" DURING THE RECENT MIDEAST CONFLICT.

ON 26 FEBRUARY, [REDACTED] CHIEF OF THE PROGRAMMING AND RETRIEVAL LANGUAGE DIVISION, WILL SPEAK ON THE TOPIC OF DATA BASE MANAGEMENT. THE TIME IS 0930. PLACE IS THE NSA AUDITORIUM.



## INTERNATIONAL AFFAIRS INSTITUTE

There will be no lecture in January. Dr. Edward Teller has accepted the invitation to speak on 5 February.



## New Officers

CMI's biennial election of officers was held on 5 December 1974. The Council, Committee Chairmen, and Executive Director are listed below. An asterisk indicates that the person is newly elected.

- REED DAWSON, P12, President
- \* [REDACTED] S1, President-Elect
- \* [REDACTED] P12, Secretary
- \* [REDACTED] N32, Treasurer
- JIM THOMPSON, A54, Council Member
- \* [REDACTED] S12, Council Member
- \* [REDACTED] R51, Council Member
- [REDACTED] S1, Council Member
- BILL MIXER, G42, Publicity
- WALT PENNEY, P15, Executive Director

## Lectures

The speaker for February has not yet been decided upon. Dr. Joseph Blum of R will speak in March, on the general subject of CHARLOW and optical processing.

## Essay Contest

Entries for the 1975 essay contest, in the form of papers on cryptology or any significantly related subject, may be submitted to [REDACTED]

or Reed Dawson, Room 3W090 (telephone 3957s), by 28 March. Any NSA employee is eligible to enter. Security classifications are permissible, but ideas or techniques originating in compartmented areas should be reduced to a noncompartmented level for entering. Technical Journal articles published during the current year will be entered automatically.

P.L. 86-36

~~CONFIDENTIAL~~

# CRYPTOLOG INDEX FOR 1974

(Listed by Contributor)

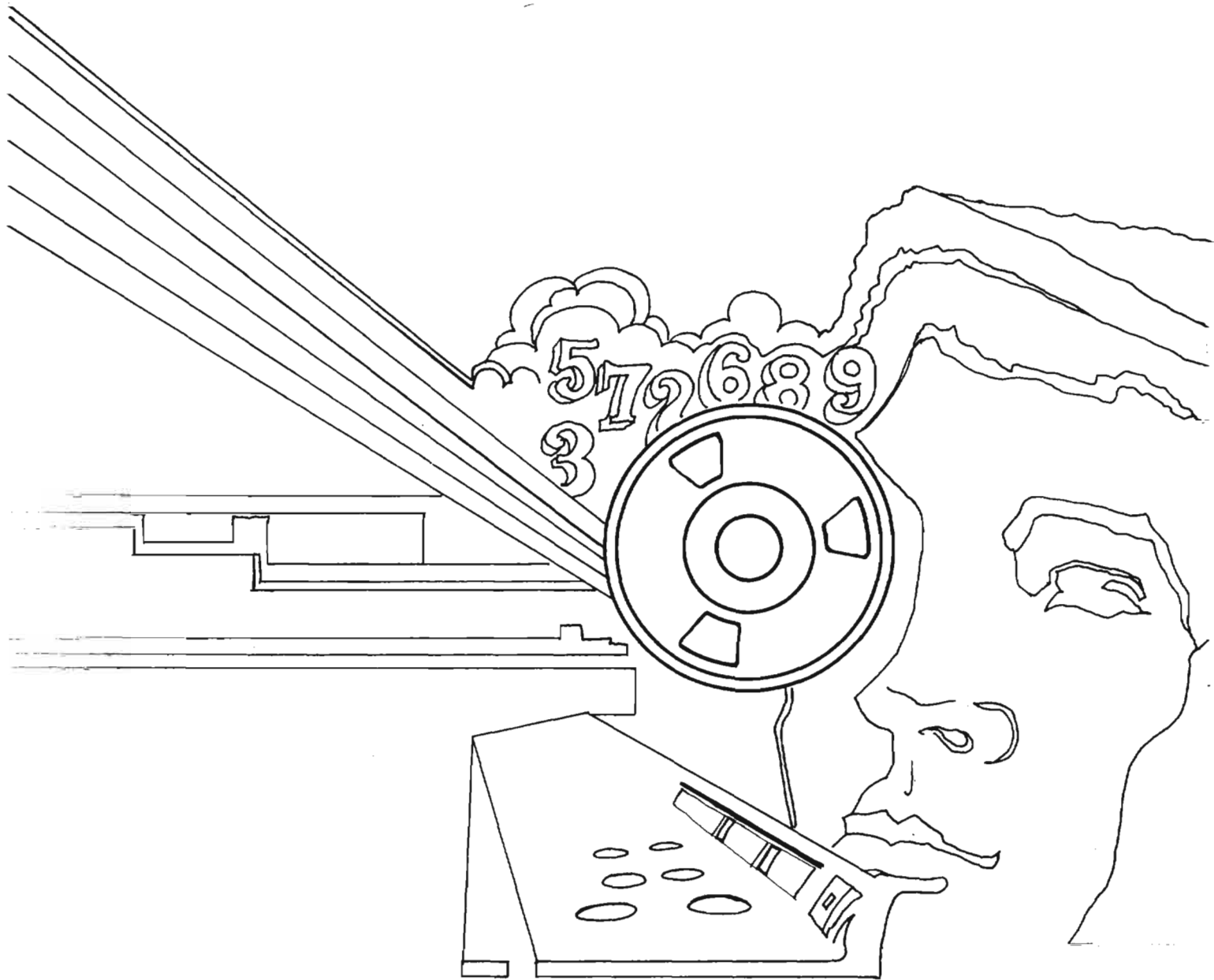
[redacted] Self-Paced Instruction: "The Future Is Now!".....Aug 15	John, George: A Flag-Waving Programmer.....Dec 13
[redacted] The Old [redacted] Section: Parts 3 & 4.....Dec 5	[redacted] Purity of the Russian Language: Slavophiles vs. Westernizers.....Nov 12
[redacted] Maps in Mind: A Photoessay.....Dec 1	[redacted] Reflections on a Translators' Conference.....Nov 10
Buck, Stuart H.: (comments in) Cryptanalysis & Code Recovery.....Sep 5 Some Thoughts on Lexicography.....Sep 11	Leahy, Francis T.: A Proposal for Calendar Reform.....Dec 19
[redacted] What Is A Collector?.....Aug 2 As We Go to Press.....Sep 7 The New Collection Criteria.....Dec 11	[redacted] King Eusyb & Queen Deodi.....Sep 19
Craig, Derek K.: COMINT Analysis of [redacted].....Sep 1	Mountjoy, Marjorie: Cryptanalysis & Code Recovery.....Sep 5
[redacted] CISI Forming New Special Interest Group on Human Factors.....Dec 10	P14: The New Traffic Analysis Glossary.....Aug 8
[redacted] The Mission of the Signals Processing Requirements Panel.....Oct 1	[redacted] Character-Building in the People's Republic of China.....Oct 7
Dudley, Barbara P.: Nice Busman's Holiday for One NSA Employee.....Aug 19	[redacted] (with Ramon Santiago-Ortiz) The Language of Beisbol in Everyday Talk.....Aug 11 Language in the News.....Sep 14 The English Language in the News.....Dec 12
[redacted] What Should You Expect? or The Analysis of Cryptanalysts.....Aug 5 Secrets of the Altars: The Moustier Cryptograms.....Sep 10 An October Overlap.....Oct 20 Answer to October Overlap.....Nov 21	Santiago-Ortiz, Ramon & [redacted] The Language of Beisbol in Everyday Talk.....Aug 11
Exinterne, Anne (pseudonym): A Long Hard Look at the Intern Program: Part One: Philosophy & Recruitment.....Sep 6 Part Two: Selection & Orientation.....Oct 11 Part Three: Motivation & Morale.....Nov 15 Part Four: What Happens to the Graduates?.....Dec 13	[redacted] Calling All SHA's: Reporting Symposium?.....Aug 20
[redacted] What? Where? Why?.....Nov 5	Tetrault, Emery W.: Even a 5-Year-Old Child.....Oct 4
Filby, Vera R.: A Spot by Any Other Name.....Aug 7 The [redacted] Exercise: A Case Study in Special Research Analysis.....Oct 16 The Apostrophe: Some Thought's.....Nov 14	[redacted] Guidesmanship or How to Write Technical Manuals Without Actually Giving Anything Away.....Nov 18
Garofalo, Caterino G.: Gary's Colors.....Sep 8	Unsigned: The New Traffic Analysis Glossary.....Aug 8 A Short Dictionary of Career Panels.....Aug 17 The Management Survey of the Philharmonic.....Aug 20 Prizes & Honors from the Learned Organizations.....Aug 21 Telephone Recall.....Oct 6 An Unofficial Glossary of Weasel Words.....Oct 10 News from the School.....Oct 14 Coming Events.....Oct 15 Assorted Editorial Notes.....Nov 4 Secret Messages.....Dec 4 Citizens of the World.....Dec 6 Letter to the Editor.....Dec 9
[redacted] Character-Building in the People's Republic of China.....Oct 7	[redacted] (comments in) Cryptanalysis & Code Recovery.....Sep 5
[redacted] Data & Definitions: Calling Things by Their Rightful Names.....Nov 1	Webster, James B.: Project CARRIAGE: Worldwide HFDF Modernization Plan.....Sep 9
Jackson, William J.: TDB: The TEX1A Data Base.....Aug 4 An Approach to Callisign Analysis.....Dec 7	[redacted] Subject: SRA Symposium.....Oct 19
[redacted] New Trends in the Teaching of Cryptanalysis: A Walk Through the '75 Curriculum.....Nov 7	Wolff, Maj Gen Herbert E.: A Letter of Introduction.....Aug 1
	[redacted] Right-to-Left Text Sorts Are Not Impossible.....Aug 14

P.L. 86-36

P.L. 86-36

~~CONFIDENTIAL~~ HANDLE VIA COMINT CHANNELS ONLY

~~TOP SECRET~~



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~