~~TOP SECRET~~

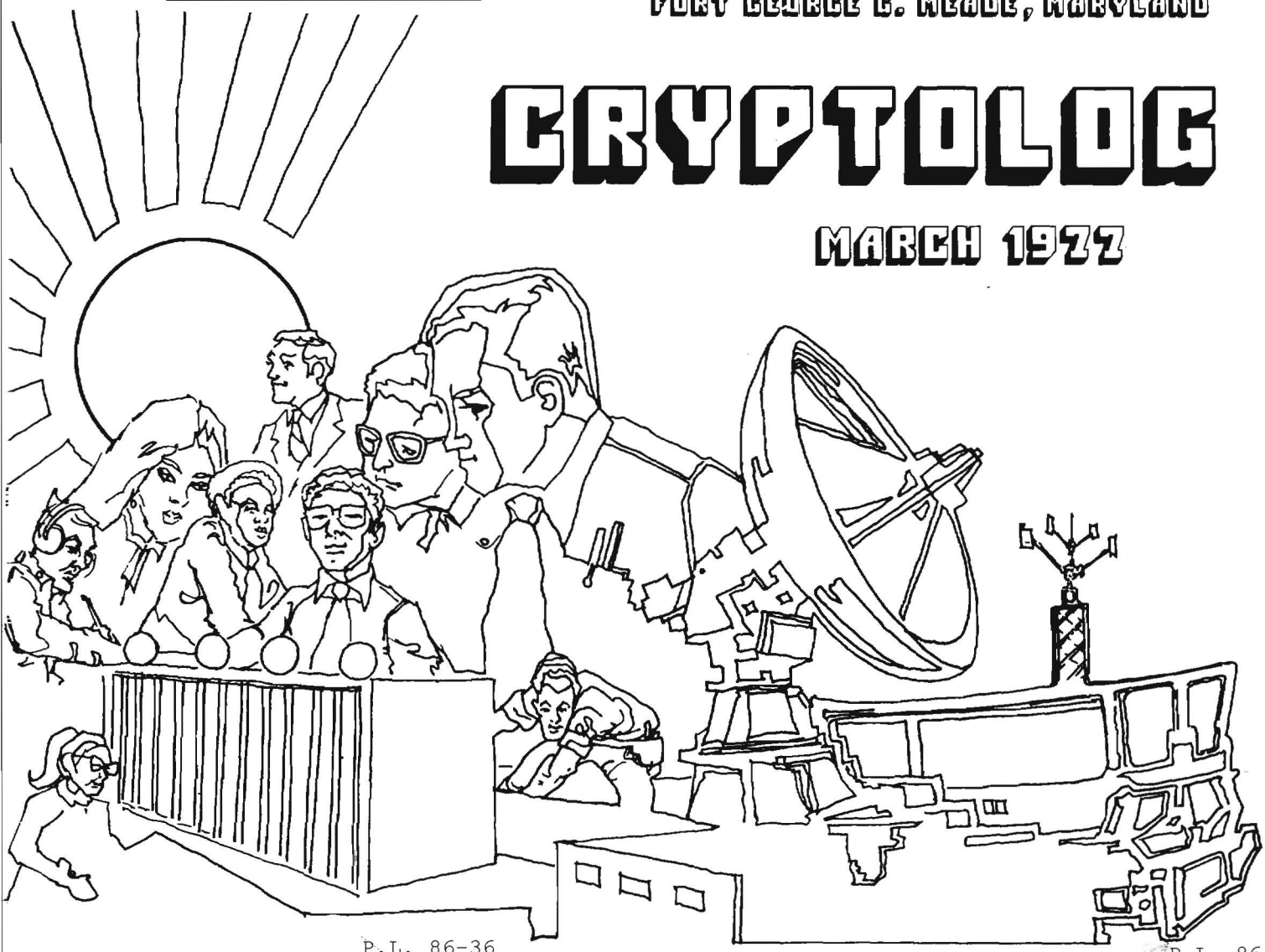
P.L. 86-36

P16 [redacted]

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MARCH 1977



P.L. 86-36

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

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

~~TOP SECRET~~

CRYPTOLOG

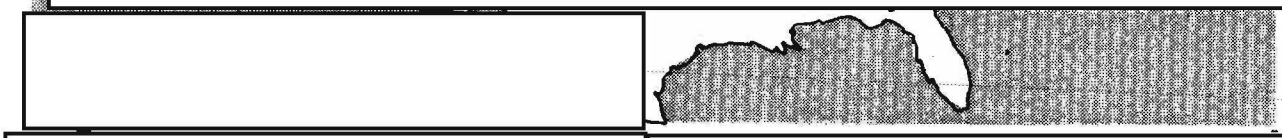
Published Monthly by P1, Techniques and Standards,
for the Personnel of Operations

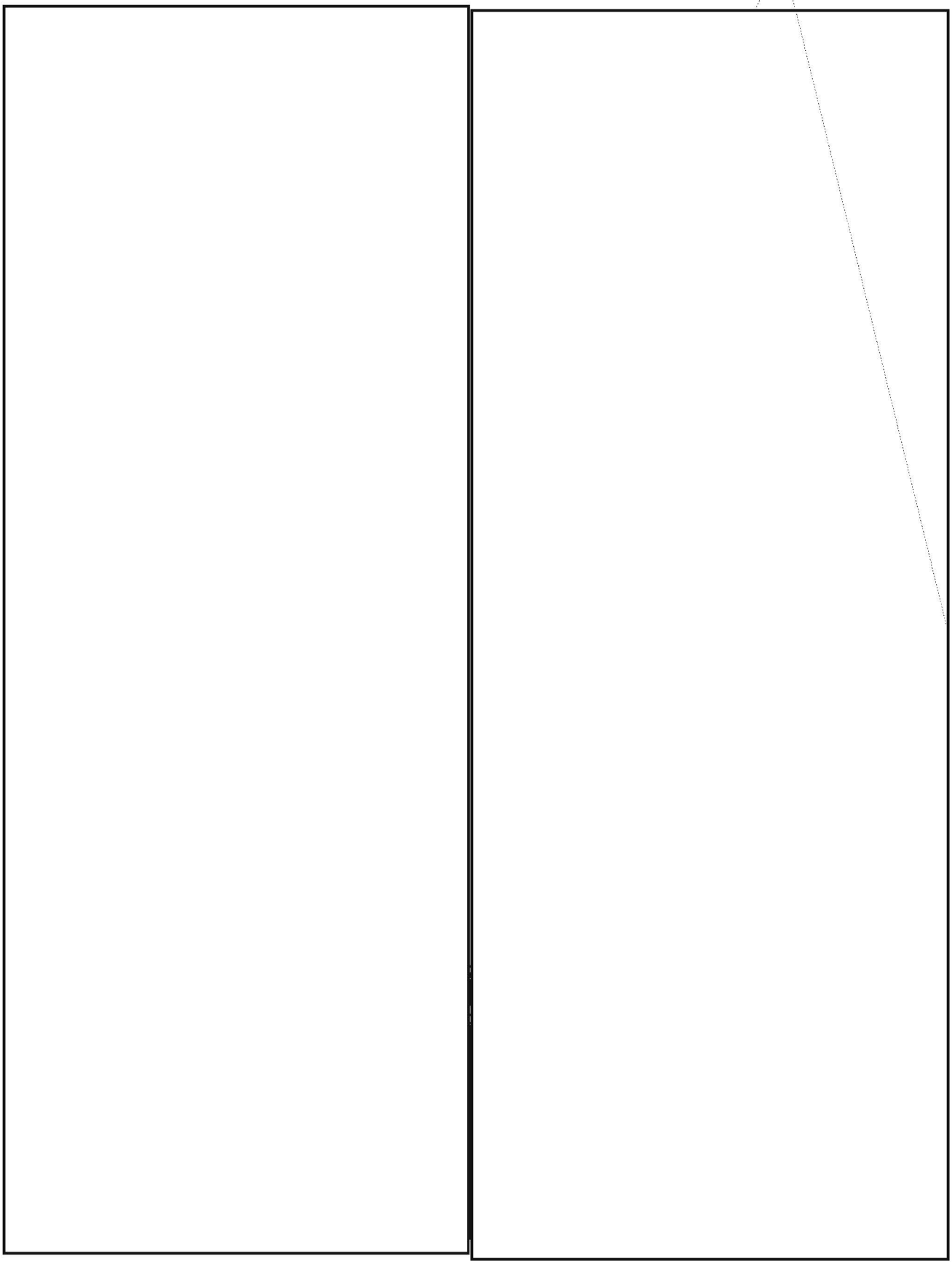
VOL. IV, No. 3 MARCH 1977

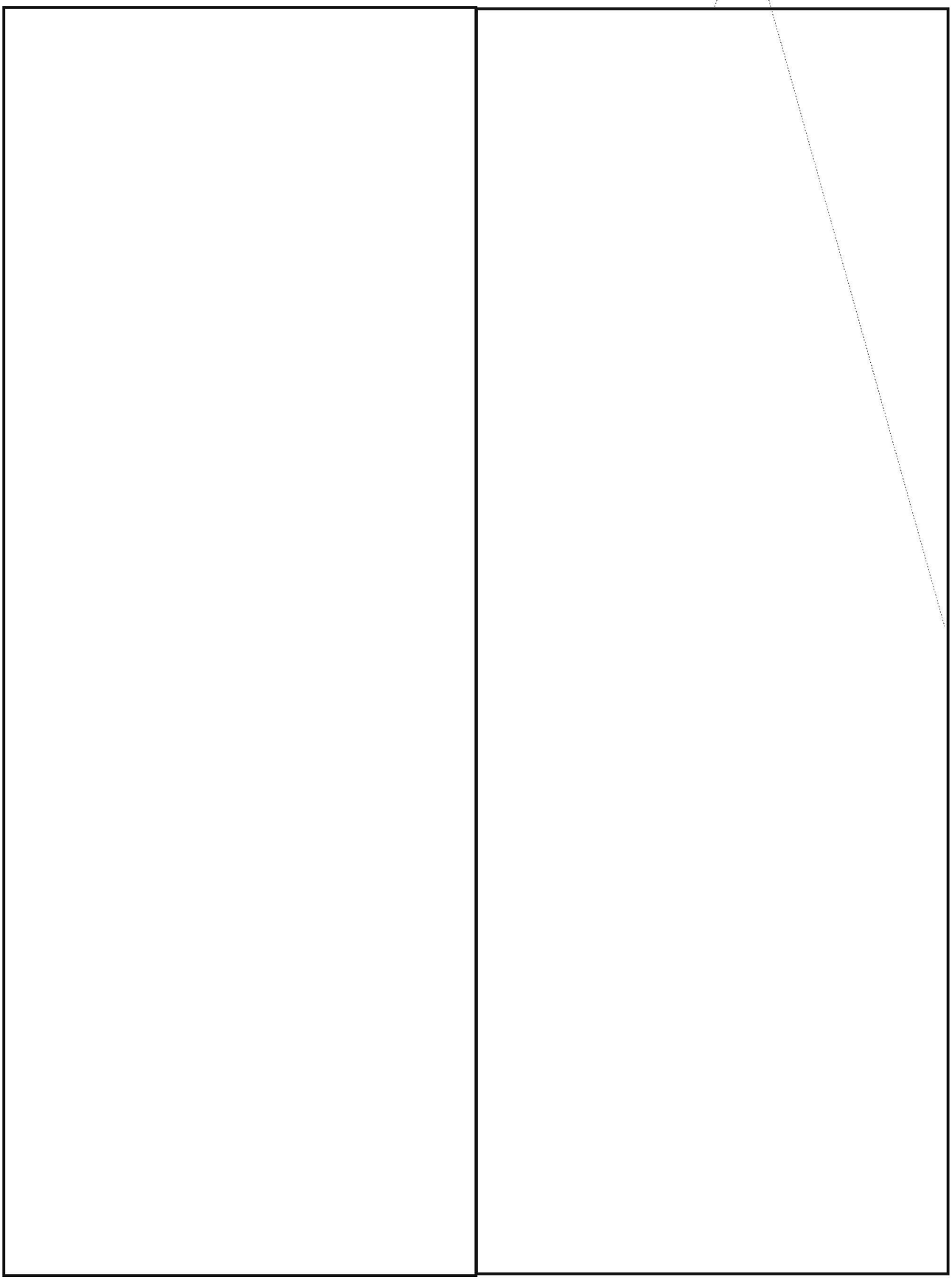
For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1

~~TOP SECRET~~

AN OVERVIEW OF PROJECT

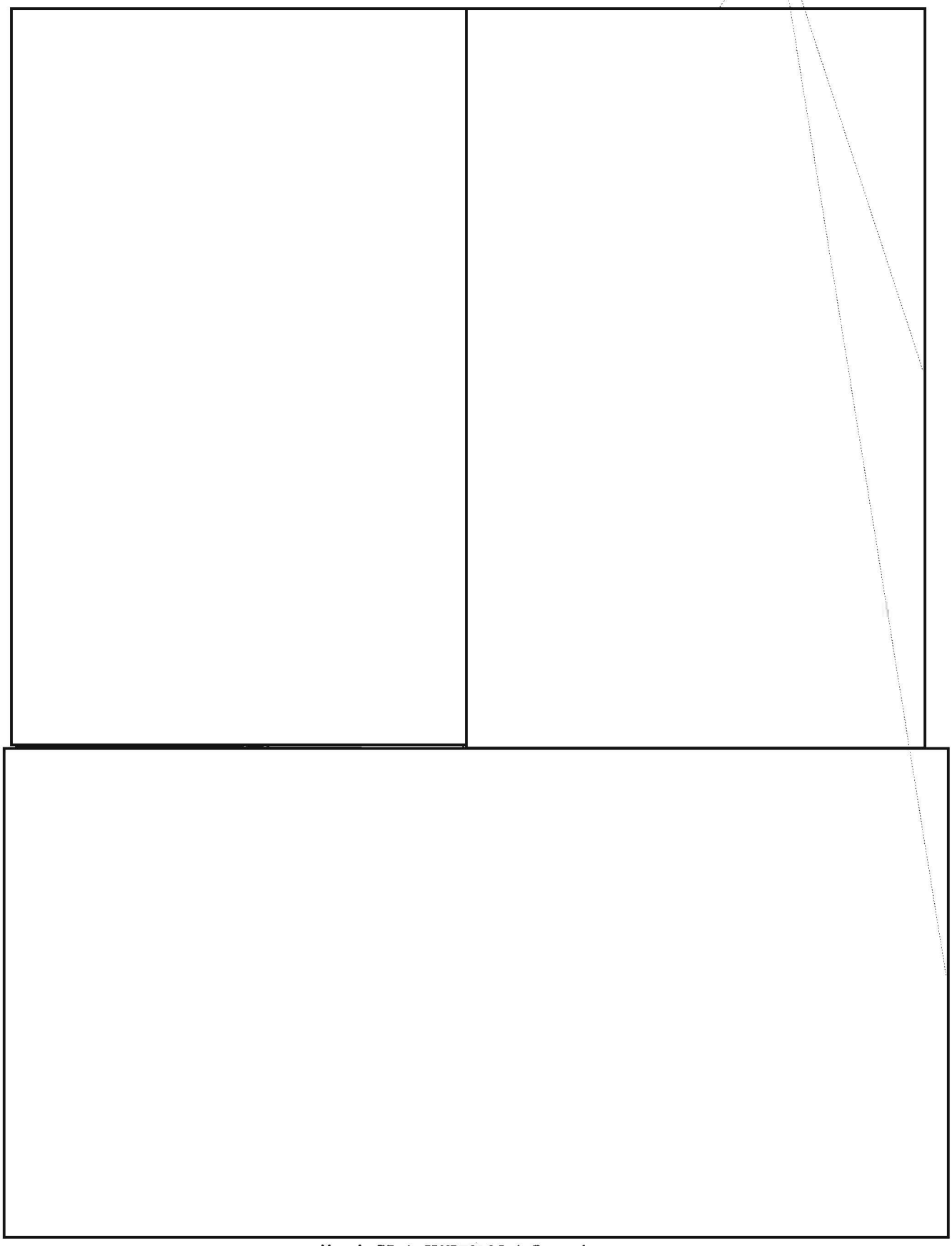


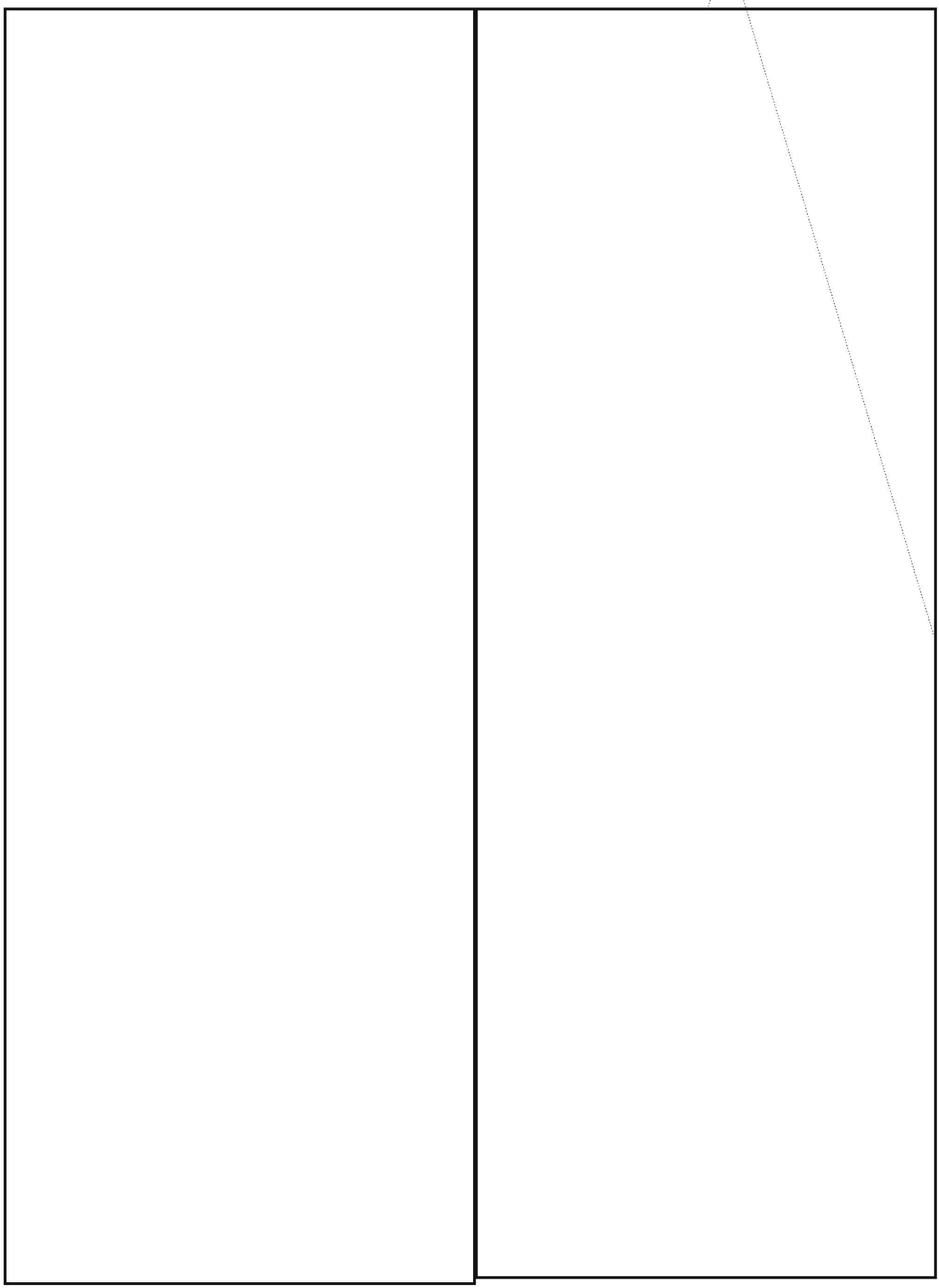


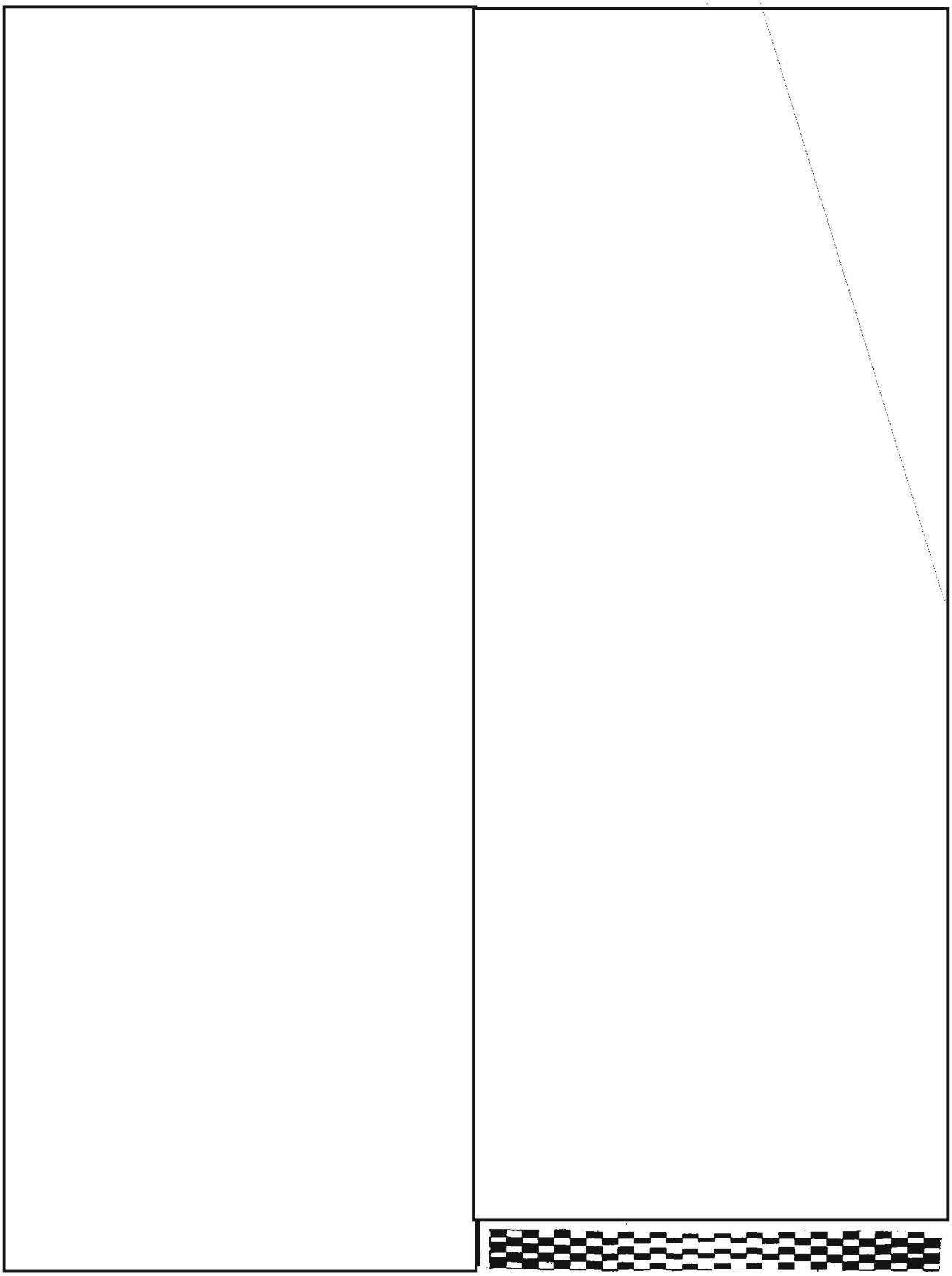


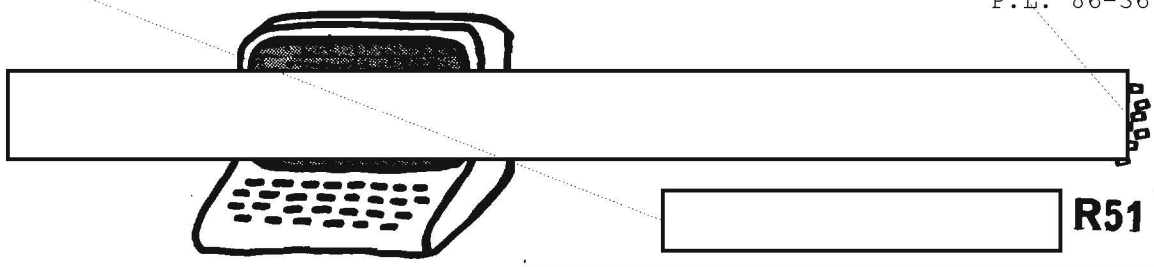
~~SECRET~~

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









R51

[redacted]

[redacted]

~~(TOP SECRET UMBRA)~~

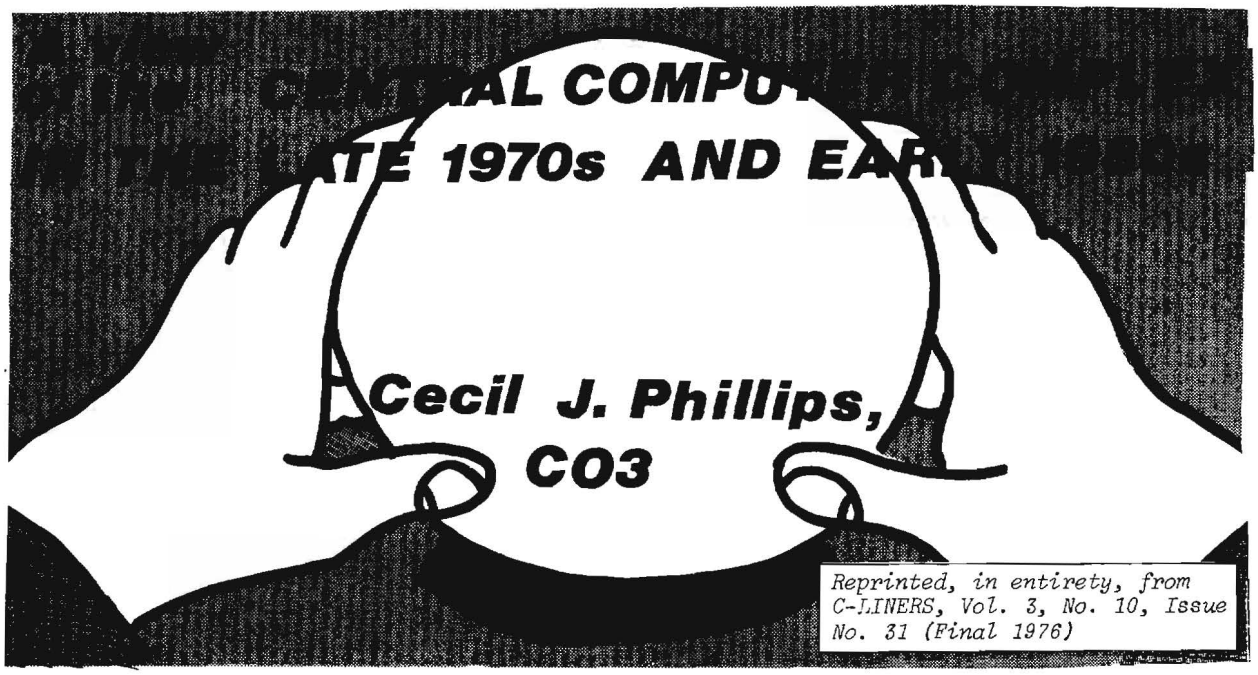
REVISED TECHNICAL SIGINT PUBLICATION MANUAL IN PREPARATION

V.R. Filby, E12

It is well known that not all analysts everywhere get to see the formal instructions and other documents that affect them in their work. For those who may not find out about it through normal channels, here is news of a document all analysts and reporters should take the trouble to get hold of and study. The revised and updated *Technical SIGINT Publication Manual (U)*, to replace the present TSPM dated 19 August 1969, is in final draft form and should be ready for distribution in mid-1977. It will be promulgated by USSID 200.

[redacted]

~~(CONFIDENTIAL — HANDLE VIA COMINT CHANNELS ONLY)~~



Reprinted, in entirety, from C-LINERS, Vol. 3, No. 10, Issue No. 31 (Final 1976)

The most dramatic change in SIGINT computer processing in the next few years is almost certain to come from the much wider development of man-machine interactive processes. This does not necessarily preclude growth in regular batch processing or growth in fully automatic processes, but it certainly means a strong shift of emphasis in the development of computer processing systems. Some of this emphasis comes from a desire to explore the newfound capability of interactive computing but, hopefully, most of it comes from a realization that machines alone are not nearly as effective as man and machine working closely together. These views are presumably not unique to the SIGINT process, since comparable growth in the use and sale of interactive computer terminals is being experienced in all kinds of pursuits.

Interactive computing in the SIGINT case can mean a variety of things. It can mean the ability of an analyst to "adjust" the collection process while it is going on. It can mean the ability to scan some output in real time and adjust it as necessary. Or, in an analytic process, it may give a person the ability to correlate and cross-check new data against the mass of historical information one has collected before; or the ability to prepare reports, gists, and similar inputs to other processes.

It is clear that there are a number of ingredients to a good interactive processing system. One of the most critical of these ingredients is a knowledgeable and well-trained cadre of users. This group is already growing, but more specific action will be necessary in the future to insure that we use the full potential of the systems which are built. At the same time, the central computing service must do everything it can to make user interfaces simpler, rather than assume that every user has some skill and knowledge as a programmer. In addition to making computer systems easier to use, the central computing service must provide a number of capabilities and tools for the users, in much the same sense in which utilities are provided to homes and businesses.

In a practical computer sense we see this utility as:

- an adequate set of computer terminals to serve all users who need access to the system and simplified user procedures;
- on-line mass data storage systems and data management software which will minimize the complexity of the user interface;
- a computer network connecting all SIGINT locations which will enable us to put the required computing power into a connected system and provide user access to any part of the system from any terminal; and
- individual computers and devices and appropriate software which will provide the best computational capability available.

Some of the details of current plans and broad concepts of usage for parts of the system are described below. This detail will be added to and modified as necessary to reflect requirements developed under [redacted]. The [redacted] overall [redacted] plan, which is basically the plan for the central computing facility and externally connected computer nodes, is due to be completed in draft early in 1977. P.L. 86-36

Computer Terminals and Terminal Access Systems

The largest group of computer terminals for SIGINT operations will consist of alpha-numeric

displays and associated keyboard for analyst interaction with the system. By 1980 or sooner, computer terminal density should have reached the point where there is at least a terminal for every three or four production personnel. This should mean that almost every analyst does part of his work at a computer terminal. A smaller set of terminals will have "full graphics" capability in addition to alpha-numeric capability, that is, they will be able to plot and to produce line drawings through the use of vectors. A still smaller number of remote batch terminals will continue to be used to initiate batch processes and to receive printed output. It is probable that as the use of interactive terminals grows, remote job entry terminals will become more basically "remote job output" terminals, or, simply, remote printers. Softcopy displays, that is, writing output to a computer file for subsequent examination on a terminal screen, will probably replace some print, but it is not too likely that all printing will be replaced. In many cases, line printers will be associated with display terminals so that output can be recorded. Equally, local storage cassettes may be used as safeguards against loss of data during entry and as a way of insuring the ability to input data at all times.

With present technology, and probably within the foreseeable future, the main bulk of the interactive terminals will be attached to minicomputers as terminal concentrators, and, through these, will be attached to the network and will have potential access to all of the system resources attached to the network. The actual access will be limited by absolute security constraints and by need-to-know procedures. These will be effected by both hardware and software means. Hardware controls are certain to be used to limit some terminals and may be used to identify users through badge readers or the like. Software controls will consists of authorization tables and passwords which will control a user's access both to files and to processes.

The total extent of the work to be performed at the terminal level or at the terminal concentrator is not yet determined. However, it seems most likely that, with present terminals, efforts will be made to limit them to "universal" functions. These will amount to data entry and data editing functions dealing with lines or screens full of data and probably to the generation of standard protocols for network entry and access to a specific system. If the terminal "intelligence" (actually storage and processing power) grows a great deal, as most manufacturers predict, then this power may be used to accomplish procedure and data language translations or to provide the capability to do other functions common to a group or class of users.

At the next, or terminal concentrator, level, more advanced functions will be performed than those at the terminal level. With controls and with standard principles applied, software in the concentrator may perform machine editing and automatic formatting, and provide file-browsing capability. Where the primary function is data entry, the concentrator will also serve as a "fail soft" capability to allow data entry to continue until the main system becomes operational again.

Work not done or not possible in the terminals or the concentrators will be done in the main systems, or "hosts." Communication between concentrators and the hosts will be via the computer network described below. To a considerable extent, hosts will be specialized processors as they are now. If network protocols and individual host protocols and language can be simplified for the user by translation and creation in the terminals and concentrators, it may result in even more task specialization by the hosts. Alternative views are that networking of host computers may result in automatic "load leveling" of tasks by automatic distribution of them throughout the network. In the next few years, the latter seems practically attainable only for multiple copies of the same computer within the network. In general, the network will contain multiple copies of hosts for reliability and backup and for achieving the desired processing power.

All of the description above pertains to user-to-computer communications through terminals, concentrators, and computer hosts, natural parts of a man-machine process. A quite separate kind of communication capability will exist within the network to support person-to-person communications. With this capability, analyst-to-analyst discussions such as are now handled by OPSCOMMs would be straightforward. A "mailbox" variation of this capability would permit messages to be left by one analyst for another when direct contact is not possible because of working time differences, etc. By signaling his "mailbox," an analyst receives all his accumulated messages from other analysts or computer generated messages to advise him of the status of some piece of work.

Data Storage and Data Management

In discussing a processing system for SIGINT operations we are certainly talking about a system serving several thousand people -- probably more than 10,000 when the operational aspects of field sites are considered. Even if terminal density is as low as one terminal for each ten members of the operational community, it will clearly be a very large system with many terminal systems and many hosts. In all probability, terminal density will be much higher, particularly so if MAROON SHIELD concepts extend to all sites.

To support such a large community of users from interactive terminals, it will be extremely important to have a large amount (if not all) of the recent data on-line. While it

is not out of the question to have a single large central store for all data, recent experience would seem to indicate that distributed data "collections" are much more likely. Some systems will have much more storage than others because of the historical nature of the kinds of problems handled and because the primary impetus in developing and marketing very large mass store systems is toward IBM systems. Thus, it is likely that we will have "unevenly distributed data," with more than half of the data in a single large collection.

Examples of this uneven nature of data distribution are quite pronounced now and will be greatly exaggerated when the IBM storage system called OAK is added to the present IBM 370/168 complex. With its 169 billion byte storage and "virtual disk" concepts, it is bound to lead to a large imbalance in storage of data throughout the general purpose system.

In spite of the imbalance, there will be a continuing need for large local collections of data on other hosts in the central complex in order to satisfy specific requirements for rapid response and other special requirements. In addition, there will be requirements for data correlation-fusing-updating and other functions inter-host. For this latter case and for inter-host/inter-process operations, a great deal of data management is needed.

We feel that a number of things will be necessary in order to deal with distributed data. First, some kind of data management plan will be desirable so that data will not be distributed helter-skelter over several storage devices. Such a plan should address necessary and unnecessary redundancy. It should also address the software tools which are to be provided to enable users, data base administrators, and others -- as well as programs and computer systems -- to have convenient access to the data. Some work has been done in NSA toward developing a data management plan (DAMAP) but clearly a great deal more work remains to be done, especially if anyone is to make regular use of distributed data bases. To a great extent we will not have very much experience with trying to use distributed data bases until the computer network linking computer hosts is operational.

As far as data base management systems (DBMS) are concerned, these are key "tools" for handling data. Hand in hand with DBMS usage, there must be a growing awareness in user organizations of the need for individuals who know the data base and control its development -- generally referred to as data base administrators. The data base administrator and his management have the potential to make data base operations useful and productive. In their efforts to do so, it is imperative that they achieve standardization of data elements, standardization of data codes, and standardization of files in the sense of requiring basic data elements in there. Data dictionaries and data directories will be key tools for data base administrators and others who face the job of producing and managing the data bases.

In achieving the SIGINT operations processing system, data base management techniques will be guided by a unified systems discipline with a goal of a single data base management system. Standardization will play a much larger role than in the past. Until adequate data standards are developed, existing data management will be continued but its future growth will be limited. The goal is a coherent whole for managing data, supported by a comprehensive set of data management tools.

Experience with networks such as COINS points to the critical need for accelerated work in NSA's data standards, Emphasis should be on NSA or SIGINT data standards, rather than large efforts at meeting non-SIGINT standards. These may be important in some cases, but many of them have little bearing on SIGINT problems. Further, SIGINT data standards work should concentrate on the most frequently used data elements and types, so that the benefits are maximum. Standardizing data elements which are rarely used or used in narrow areas of SIGINT is useful, but it does not contribute as much to the areas of broad use.

A final note on data standardization implementation -- a phase more difficult than developing the standard. This must be vigorously but rationally pursued, with NSA management taking active interest in the arguments and counterarguments. Good standards are usable standards.

Computer Networking

Another key ingredient of a large interactive system such as that required by SIGINT operations is a way of linking computer systems. The scope of SIGINT processing exceeded a single large computer many years ago. In the interim, specific computer-to-computer linking and loose coupling of several large computers through shared storage have helped with the problem. Project [redacted] NSA's computer networking plan, is the generalized solution to linking as many systems as necessary into an integrated processing complex. P.L. 86-36

Project [redacted] may be described as a "railroad," since it provides the basic techniques for linking computers and terminals with standard connection protocols. It does not of itself guarantee standard processes, standard data bases, or any other set of standards except for the basic network protocols. P.L. 86-36

NSA's computer networking is based on technology developed for the Department of Defense Advanced Research Projects Agency (ARPA). It is a packet switched network in which every node is connected to at least two other nodes. This gives additional reliability to inter-host connections. As mentioned above, the use of these

connections is not controlled except by the network protocols, network control programs in the hosts, and the provisions for inter-process communication.

As the network comes into use, some additional controls will come into use. Security will be one of these. Job, process, and message accounting will add another dimension of control. The details of an overall control or management system are yet to be developed, but will be formed from the experience of using the network and from growing user requirements for process control or process management. The requirement for process management by users is developing rapidly in parallel with the ability of processes and processors to be linked together.

Effective use of the network will require extensive user knowledge of computer processes and computer facilities, as well as knowledge of the data mentioned earlier. A network information center is being developed to assist the users in understanding all the capabilities and complexities of the network.

The full development of the computer network [redacted] will take a number of years. Its effective use is a key factor in the development of the Agency's potential to use computers.

The Equipment Complexes

Equipment complexes (or sometimes "computing complexes") is a term which has come into increasing use as we couple two or more pieces of equipment or link equipments through some common peripheral device. The use of equipment complexes for planning and management has been accelerated by the need for operator and maintenance economies, and by the practicalities of consistent operation of identical and related systems.

The principal example of such an equipment complex is the main IBM 370 complex, now called [redacted] By developing the large IBM systems so that they share disk storage, a significant improvement was obtained in the flexibility of the four systems. At the same time, it was possible to reduce the staff necessary to operate the machines. In other cases, we can also reduce maintenance costs by collocation of machines.

The Central Data Processing Complex [redacted]

This complex is the historical successor of more than 40 years of automatic data processing (ADP) which began with IBM punched card machines in the 1930s. As noted earlier, it is the processing area where the most data is stored and where the input and output (at least of traditional data records) greatly exceeds any other set of NSA computers. Because of storage capacity available in this complex, and because of increasing requirements for data correlation, this complex continues to grow at a considerable pace. It is possible that computer networking will reduce the demand ". . . to have everything together," but from a practical point of view this will take some time, perhaps 2 to 3 or more years.

Immediate plans for the large IBM 370 systems are to add a fifth IBM 370/168 to the present four systems and to create one multiprocessor system. It is planned that the multiprocessor will serve needs which demand high reliability or availability. This will include immediate front-end processing of field data arriving from [redacted] and support of critical terminals. The whole 370/168 complex, along with the OAK mass storage system of 169 billion bytes of on-line data, will serve [redacted] and similar functions.

The present IBM 370/158 serving primarily administrative functions will be upgraded to an IBM 370/168 and formed into the larger complex by loose coupling through shared storage and by linkage to the computer network. The present IBM 370/158 used for Information Storage and Retrieval (IS&R) will serve principally as a developmental system and will be used in background mode and in nondevelopmental times for large batch processes. Future large IBM systems (or IBM-based systems such as AMDAHL) which may have to be added as supply capacity will be coupled into the main complex. The linking of more systems as multiprocessors will be dependent on the success of the MP system planned for late 1976. P.L. 86-36

In order to meet DDO's goal by bringing time-critical and batch processes together, the IBM 370 complex will have to be made to respond much more rapidly, so that bulk data can be almost as available as selected data such as [redacted] reports. In fact, it seems likely that [redacted] and the IBM 370s will have to work well together to accomplish this.

The Time Critical Complex

This complex is also expected to continue to grow rapidly. The success of the TIDE system over the last 6 or 7 years has produced the present overload state of the pair of UNIVAC 494s and has led to the development of PREFACE plans.

As planned, the UNIVAC 1110s in [redacted] will be used to relieve [redacted] of processing functions, as distinguished from communications functions. While converting processes from the U 494 to the U 1110, a data base management system (DBMS) will be introduced to provide for more orderly handling of data and to simplify future programming. As the [redacted] development proceeds, it will be necessary to address the broad question of alpha-numeric terminals for NSOC and to begin development of plans for a communications subsystem to replace [redacted]. It is estimated that [redacted] will continue to operate until at least January 1980, and possibly a couple of years after that.

P.L. 86-36

[redacted] which is now slated to serve both full graphics needs and some alpha-numeric needs, will be diverted to full graphics-only usage as [redacted] becomes operational. A careful study of all full graphics needs will be undertaken with a goal of developing a set of requirements for full graphics. While these requirements will ultimately drive the full graphics solution, it is likely that [redacted] will fill most of these needs over the next 2 to 4 years.

The High Compute Complex

This complex of computers is now almost entirely synonymous with cryptanalysis. To some extent this is because the cryptanalysts have carefully guarded it and to some extent it is because the [redacted] set of CDC 6000s preceded the first CDC 6600 for cryptanalysis.

As far as the cryptanalytic side of the problem is concerned, the high-compute-complex plans are described under a C Group concept called HYPERCAN -- for *HI*gh *PER*formance *C*rypt*AN*alysis. Under this concept, four CDC 7600s using the NSA/IDA Operating System will be linked by a 50 megabit data transmission bus. In addition, a new and more advanced super computer [redacted] will be sought to add to the capacity of the complex. We hope to add this new capacity in about 2 years and, thereby, double the straight-compute capacity. Interactive terminals will not be developed at the output for the new system. Instead, access to the new system will be primarily through the CDC 7600s and the 50 megabit network. This is expected to optimize the use of available resources and to minimize the impact on users by retaining the present NSA/IDASYS procedures and languages.

Operating Facilities

The term "operating facility" is being used as a catch-all for the NSA end of remoted collection operations. Presumably, every one of these operations needs some interconnection to the main computer complex. To date, most of the interconnection has been described as a connection to the computer network -- [redacted] with little more specifics than that. Almost without exception, design of these complexes has ignored the necessary and desirable interaction with existing data collections on the central computers. In viewing overall operations processing in the next few years, it seems certain that more complete plans will have to be developed using existing resources as well as the new equipment.

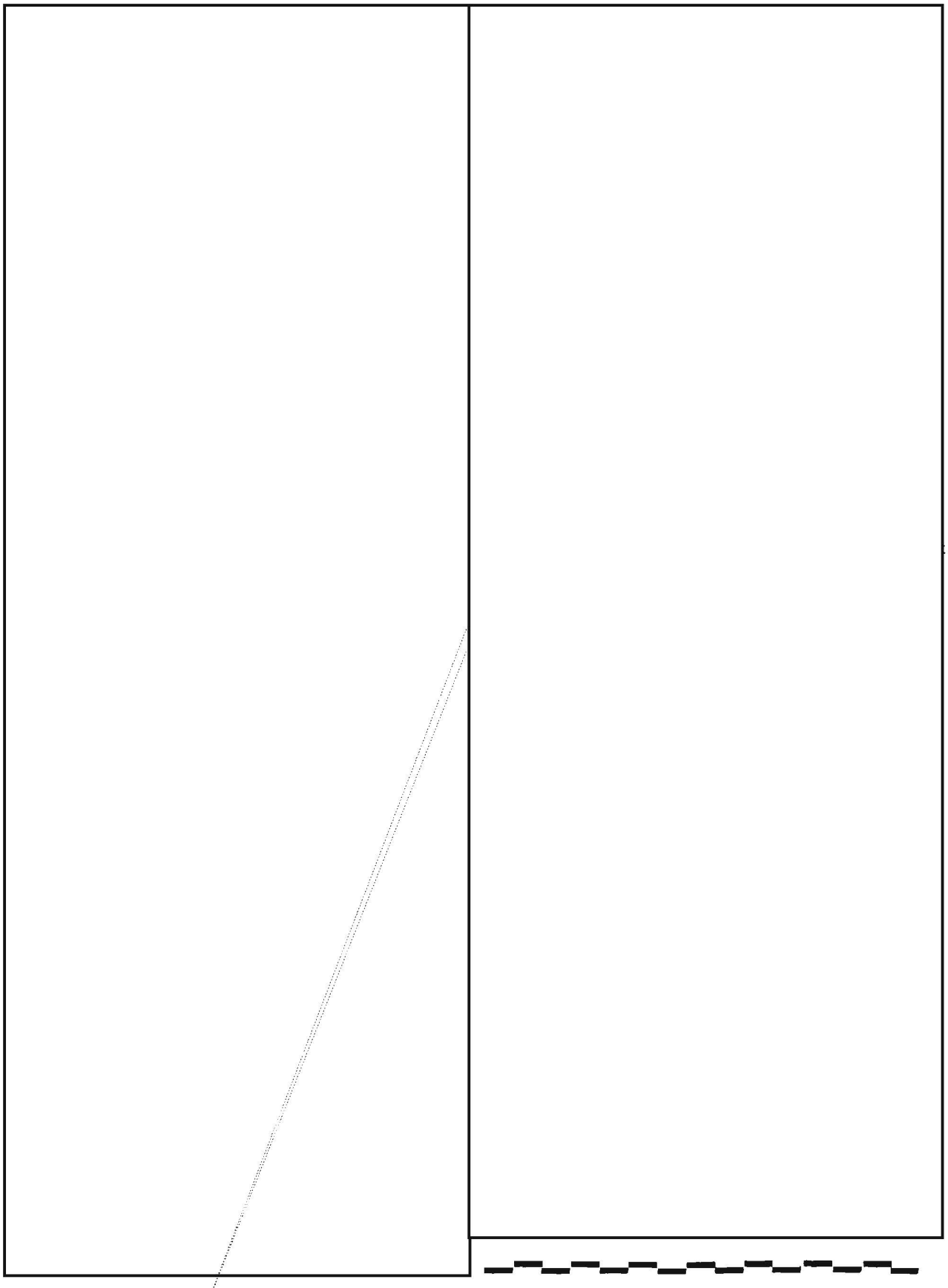
One mode of operation which may emerge is to limit "operating facility" computers to problems requiring extremely quick response and to use the main computing complex (MCC) for basic support. In this mode, the MCC would update basic files in the operating facilities by "downloading" from the central analytic files. In the operating facility, immediate response problems would be dealt with by the local computer and more complex questions could be relayed to the MCC. This mode is already projected in [redacted] applications where the broad functional similarity to Morse collection is almost identical, except for tuning.

The presence of high bit rate signals at operating facilities may dictate the need for a special network or data bus paralleling the [redacted] network. This is under study in R as a part of [redacted] and other projects. It is most likely that [redacted] would be used for control information and that the parallel high-capacity linkage would be reserved for only signals. This would limit the number of required nodes.

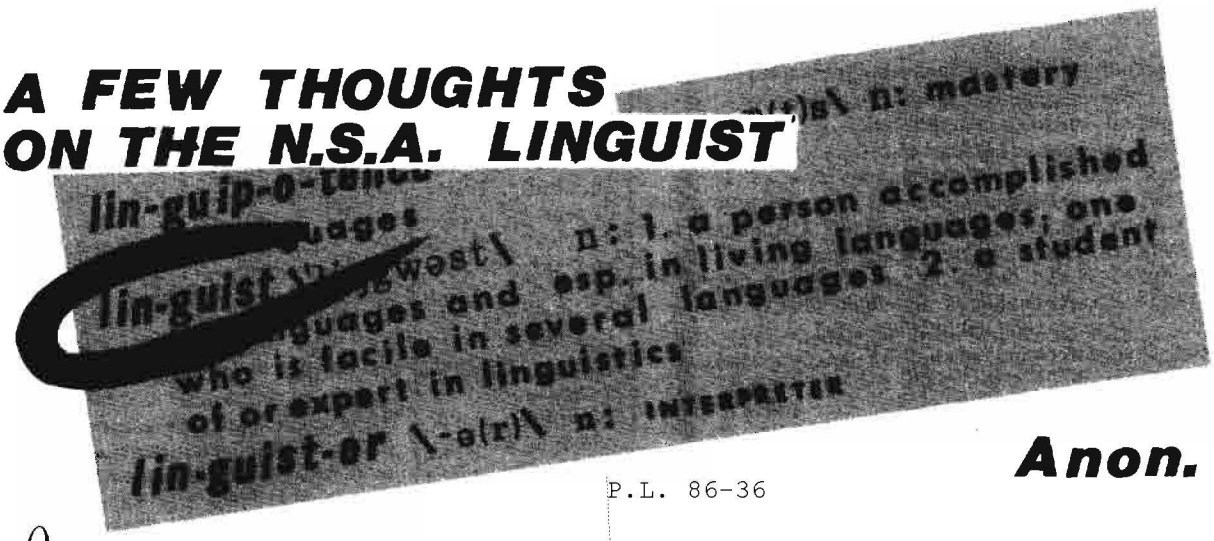
More details of these connections to the [redacted] network and the interaction of operating facilities with the Main Computer Complex are emerging as the projects develop. It is reasonable to expect that requirements gathered for [redacted] will provide more understanding of what is needed.

[redacted]

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



A FEW THOUGHTS ON THE N.S.A. LINGUIST



Anon.

P.L. 86-36

I am being somewhat arbitrary in using the term "linguist." What I mean here is an individual who is capable of performing the full range of tasks required at NSA in which knowledge of a foreign language is *primary*. Let's forget all hyphenated job titles in which some degree of language knowledge is coupled with some other skill. You can carry this hyphenation business to the point where it becomes difficult to locate *anyone* who doesn't claim to use a foreign language to some extent in his or her specialty. It sometimes seems that the pretensions of such people are in direct proportion to their ignorance of the language claimed.

Nonlinguists, especially, have a curious tendency to treat language jobs as though we at the Agency were in complete control of inflowing language materials. Thus, a particular language task (in a very low grade, of course) is described as "highly stereotyped, low-level," requiring no more than a minimum language knowledge.

[redacted]

So, what is a linguist expected to know -- everything? It would be a miracle indeed to discover a native of this country who has mastered his own language (including all the words in the dictionary), and, besides that, knows all the subjects that can be discussed in English; in short, a walking encyclopedia of both linguistic and factual information. Obviously, there is no such person. It should come as no surprise, then, that the NSA linguist at any level is apt to run into problems that involve either language or factual knowledge (or both) outside his own experience, not covered in any of his training courses or anticipated by the latest crop of "scientific" linguists -- and not to be found in any reference works available to him. If we agree that it is extremely important in our work to be right [redacted] if you doubt this), what, then, can you reasonably expect of an NSA linguist? What choices do you offer him? Must he confine himself strictly to the level of his job description (and pay), and ignore everything else? Or should he try to cope with everything that flows across his desk, even though many of the problems (linguistic and otherwise) will be beyond his competence?

Backing off for a moment, let's consider again the first question raised: what *is* a linguist, anyway? Is he a person who can provide a precise description of a language, employing all the scientific terminology currently in vogue? Or is he someone who can use the language as an educated native would? Is it realistic to assume that the person who can describe a foreign language can also *use* it in the manner indicated? Probably not. Of the two, which one does the Agency's work -- the "describer" or the "practitioner"?

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

I am reminded here of the never-ending debate over the term "bookbreaker." Is he (or she) the person who "breaks into" a code and provides a tentative description of its size and structure -- with, perhaps, a few hypothetical "recoveries"? Or is the bookbreaker the one who actually *reconstructs* the code book to the point where incoming messages can be decoded and translated upon receipt? I would go

[redacted]

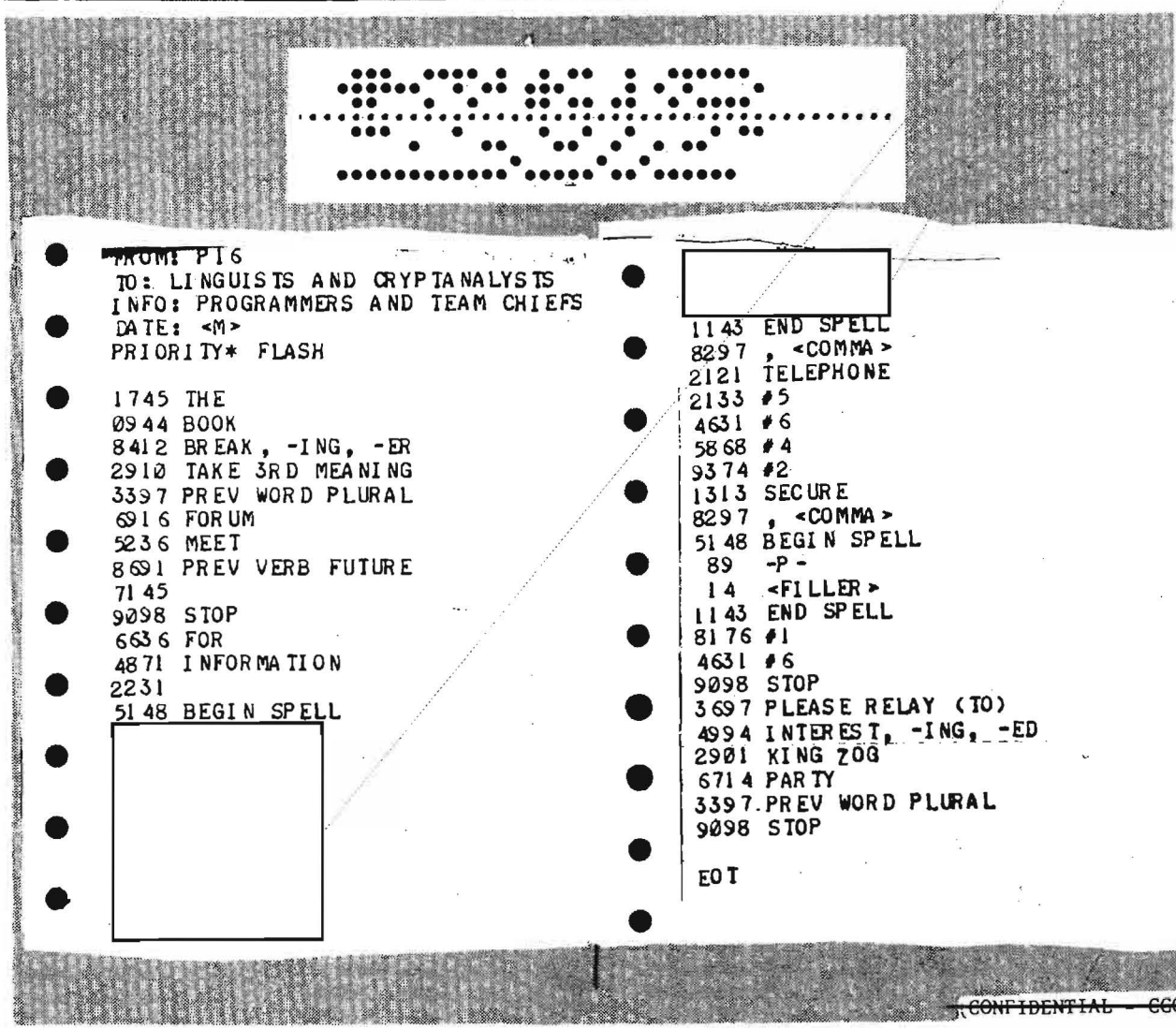
P.L. 86-36

even further and insist that the "reconstructor" should, upon request, be capable of translating any decoded message -- and have his translation survive a language check by the most experienced linguist in the area (who may not be friendly). A demand like this tends to divide analysts into two groups: the "describers" and the "reconstructors." These two groups will disagree forever as to who is more deserving of the title "bookbreaker," but that isn't the point. Their great debate is really more over status than anything else. In my own mind, I expect as much of the "code reconstructor" (the one who meets the standard imposed above) as I would of the true NSA linguist, as defined at the outset. Neither one has the right to assume that the task at hand will be tailored to fit his own limitations or narrow interests. To begin with, both must be literate in the foreign language involved ("literate" as defined in Webster's -- "able to read and write").

Why make such a big thing about mere literacy? Simply to plant our feet firmly on the ground in this whole matter. We shall never get the linguistic paragon who knows all the answers offhand, nor can we afford the risk of depending forever on those who never know enough. The real NSA linguist is the person who is literate to begin with -- and who has an infinite capacity for growth. To quote Will Rogers, "We are all dumb on certain subjects," and this description fits linguists like a glove. But with the ability to read a foreign language at sight, we can overcome our ignorance by searching for the answers in the very places where a native scholar would look, just as we regularly consult standard reference works in English. If we still can't find the answers, the trouble may be that the other fellow's reference sources are better than ours.

P.L. 86-36

~~(CONFIDENTIAL - CCO)~~



FROM: P16
TO: LINGUISTS AND CRYPTANALYSTS
INFO: PROGRAMMERS AND TEAM CHIEFS
DATE: <M>
PRIORITY* FLASH

1745 THE
0944 BOOK
8412 BREAK, -ING, -ER
2910 TAKE 3RD MEANING
3397 PREV WORD PLURAL
6916 FORUM
5236 MEET
8691 PREV VERB FUTURE
7145
9098 STOP
6636 FOR
4871 INFORMATION
2231
5148 BEGIN SPELL
[redacted]

[redacted]
1143 END SPELL
8297 , <COMMA>
2121 TELEPHONE
2133 #5
4631 #6
5868 #4
9374 #2
1313 SECURE
8297 , <COMMA>
5148 BEGIN SPELL
89 -P-
14 <FILLER>
1143 END SPELL
8176 #1
4631 #6
9098 STOP
3697 PLEASE RELAY (TO)
4994 INTEREST, -ING, -ED
2901 KING ZOG
6714 PARTY
3397 PREV WORD PLURAL
9098 STOP

EOT

~~(CONFIDENTIAL - CCO)~~

P.L. 86-36

[redacted]

The year, 1965. The place, the NSA SIGINT Command Center. The occasion, the beginning of the NSA SIGINT Summary. And you are there . . . (Sorry, Walter!)

The May 1976 issue of CRYPTOLOG contained an article by William Hunt, SA/DDF, which described in some detail the functions and purposes of the NSA SIGINT Summary. On the whole it was rather complete and quite interesting. But for the period between the inception of the SIGSUM and Bill's association with it -- a period of 8 or so years -- the article provided virtually no information at all. Having, with some others, devoted a part of those years to the business of conceiving and developing the SIGSUM, I am perhaps in as good a position as any to fill in the gaps. In the process, I will also clarify some statements in the article that are unintentionally misleading, made so simply by the fact that Bill had no part in the conception and early development of the report and therefore could not be expected to know how it all began.

In the early 1960s, a number of events occurred which, taken together, had a far-reaching impact on the role NSA was then playing in the U.S. intelligence community. Where prior to that time the role of the SIGINT establishment had been mainly that of collector and processor, from the Cuban missile crisis onward we experienced a marked increase in requirements for end-product reporting of SIGINT developments. Our customers wanted SIGINT information to be put in its true perspective. At the same time, of course, we were reminded to avoid even the appearance of producing "finished intelligence" for which we were not equipped, technically or statutorily. Coincident with the entry of NSA into the reporting business was the establishment of the NSA SIGINT Command Center, successor to the PROD Watch Office and predecessor to our present NSOC. At some point during this time it must have seemed logical to produce a daily summary of SIGINT highlights for our customers and for NSA executives. And so the NSA SIGINT Daily Summary (SDS) -- the immediate predecessor of the NSA SIGINT Summary -- was born.

The SDS was divided into three sections:

- World Highlights (mostly G Group items),
- Red Extract (A Group items), and
- Gold Extract (B Group items).

Items were carried to the Command Center during the morning and early afternoon, edited there, and delivered to the FLEXROOM in the early evening hours for hard-copy and electrical preparation. Later in the evening the electrical version would go out over the wires to a worldwide distribution which is essentially the same as that which the SIGSUM uses today. The hard copy, most of the time, would be delivered to its Washington-area customers early the next morning. (I say "most of the time" because I can recall one or two times when its delivery was not so early and some of our customers let us know about it.)

The SDS had some shortcomings. The quality of the items it printed was, to put it charitably, inconsistent. Items were often submitted in handwritten form and had to be deciphered

". . . the idea was not passionately embraced; at least, not right away."

and typed before they could be edited. Most serious was the virtual absence of any input to the Gold Extract. The reason for that was that [redacted] put out its own daily summary and the SDS was not only competition for it but, since a large percentage of their respective audiences were the same, there was the problem of redundancy. For these reasons, chiefly, the then deputy chief of the Command Center, [redacted], sent me on a mission to each of the PROD Group chiefs to appeal for better support for the SDS. The result of the conversations which then took place was a decision to scrap the SDS in favor of the daily report now called, as it was then, the NSA SIGINT Summary.

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

P.L. 86-36

Contrary to what one might suppose, the idea was not passionately embraced; at least, not right away. [redacted] and some others in the Command Center had reservations about the size of the effort that would be necessary. And there was some concern expressed that we would get flak from CIA, DIA, and State on the ground that we infringing on their prerogatives. But the SIGSUM was clearly an idea whose time had

come. All the Group chiefs and Chief, P05 were strongly in favor of a first-class daily SIGINT summary report, in fact, had been for some time, and persuaded the then ADP, [redacted], that the time to strike was at hand.

It took about 2 months to do the preliminary planning for the SIGSUM. The original team that was responsible for developing the format and layout consisted of two people -- Dave Cossum and me. Warner Parsons soon joined us as visual-aids coordinator, and [redacted] and [redacted] were the principal artists who developed the cover design and page formats.

At this point it should be made clear that the SIGSUM had no official status as yet; Mr. [redacted] had only given his approval to explore the ways and means of upgrading NSA daily-summary reporting and to prepare a mockup (a printer's dummy) of our proposed publication. He would then decide between two alternatives: seek the Director's approval or shelve the idea. In the course of the exploration some amusing situations developed. The one that I remember most clearly had to do with estimating the number of maps we would have to keep on hand to cover all reasonably projected reporting situations for a given period of time -- 2 months, I think. Our plan was to place the resulting order with a Mr. [redacted] at CIA, with whom we had a "connection." After considerable postulation, speculation, and multiplication, Warner arrived at a number that none of us, including him, believed. Our astonishment was quickly exceeded, however, by the uproarious laughter the number evoked in our "connection," [redacted] then Chief of the Geographic Branch in CREF (now C5). The number was 1,500,000 maps. (Incredible as it may seem, the figure proved to be very near the mark.)

EO 1.4.(c)

[redacted]

At this point I must take issue with Bill on three points he made in his article, and clarify the situation by emphasizing the following true statements:

- the SIGSUM was *not* conceived and designed by the Assistant Director for Production;
- there *was*, indeed, a clear-cut requirement for it which was set forth with admirable clarity and directness by General Carter in a letter to DIRDIA, General Carroll, in early 1966; and
- it *was* fully developed within a year after it first appeared.

The reader might have also concluded, if he has read this far, that it is indeed both possible and -- from my point of view, at least -- desirable "to trace the SIGSUM's growing pains."

By mutual agreement with the Group Chiefs, the SIGSUM was put together every day by an editorial board on which each Group had representation. In addition, a CREF representative, Miss Ruth Schley, provided collateral and scientific and technical information support, and Warner Parsons served as art editor.

The other charter members of the editorial board were [redacted] Dave Cossum was appointed Editor-in-Chief, and I was designated his alternate. The hard decisions which became the basic operating philosophy of the SIGSUM were hammered out by this group, often in the late hours of the evening. One of the Director's briefers, [redacted] also sat in on the deliberations. This group of people and the others who followed them, particularly Warren Keniston [redacted] deserve an equal share of any credit that is to be given for the SIGSUM. The result of all their efforts was a first-class intelligence report that was widely praised as being a worthy addition to the daily reports that were already available to the government's highest-level decision-makers. Among the many laudatory wires received, I particularly recall those sent by the Secretary of State, CINCSAC, and CINCPAC. We were also told unofficially that it was warmly received at the White House (a number of copies with Walt Rostow's marginal notes very much in evidence were mysteriously returned to us for disposition). Needless to say, we were all both pleased and relieved to have the SIGSUM so highly regarded, especially by some who might have considered it competition with their own daily summaries. The SIGSUM had received its baptism of fire, so to speak, and had come through it unscathed.

P.L. 86-36

> "Among the many laudatory wires received [after the institution of of the SIGSUM], I particularly recall those sent by the Secretary of State, CINCSAC, and CINCPAC."

[redacted]

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

Letters to the Editor

To the Editor, CRYPTOLOG:

I had a scare the other day, but it all turned out okay and I thought that you and some of your readers might find amusement and instruction in the tale. While on a brief TDY to [redacted] Washington, with [redacted] we were told informally, by one of the people there, of a technique [redacted] that amazed me. This was the story:

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

[redacted]

doesn't seem to matter.

Had we been missing an obvious bet? How could such a scheme possibly work? We had to find out more about it.

[redacted]

Without denying that this scheme, which has proven to be very successful, is an example of a simple yet ingenious solution to a problem of long standing, I am relieved. If it were possible to train a linguistically naive person to listen to *any* language and hear specific words imbedded in conversations, some basic ideas would have to be changed, and I am too old to start over.

Jack Gurin, R5

~~(SECRET - CCO)~~

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

To the Editor, CRYPTOLOG:

Under normal circumstances I would have exercised my prerogative to ditch C-LINER's "Impure Mathematics" (Final 1976 issue) in the open trash receptacle where it belongs. It clearly has no SIGINT value, no intellectual value, and in my judgment not a modicum of socially redeeming value. No wonder the author chose not to put his name to it.

But I can't do that because the thing was published in an official government document under an official SECRET Codeword classification -- circumstances which could hardly be considered normal. Hence, the burn bag.

I feel reasonably confident that C-LINER, in taking upon itself this one degree of freedom too many, has offended the moral and professional sensitivities of other people around the agency, as it did mine. It is inconceivable that the average mission-oriented NSAer would give assent to the seepage of this type of writing into SIGINT literature. P.L. 86-36

Where is the sorely-needed NSA/CSS voice of authority to say: "Yes. As a society we have indeed mortgaged our self-respect to the likes of Hefner and Guccione. But this is where we draw the line"?

Hopefully, we will not have to wait too long before the Director's voice is heard in this regard.

As for C-LINER itself, all things considered maybe it is just as well that it's now a thing of the past.

"Appalled"
[name withheld at writer's request]

Copy to:
Chief C (Mr. Speierman)
Director NSA/CSS (General Allen)

(UNCLASSIFIED)

Editor's reply

In the final issue of C-LINERS ("the second reincarnation cycle of the C Group Machine Processing Information Bulletin"), its editor, David J. Williams urged potential authors to send their articles to CRYPTOLOG. He also stated, "If you disagree with any of the materials in this issue, you can carry on the fight in CRYPTOLOG, I am sure that Arthur will be happy to carry your rebuttal." I'm pleased that someone took up Dave's second suggestion. Wouldn't it have been nice if someone had taken up his first suggestion that quickly.

Dave explains the lack of an author's name as follows: the item was supposed to have a headline "Tales from the Past" or "Golden Oldie"), but the headline got dropped during page composition. The general feeling was that the item was in the public domain, and might have been written by "someone [redacted] in the early 1950s." Dave says that he is "highly EO 1.4.(c) P.L. 86-36

amused" at the reaction it evoked from you because, when the C-LINERS editorial board was considering it for publication, they showed it to several professional mathematicians. All felt that it was (a) "cute," (b) "professionally sound," and (c) "definitely worth printing." With a consensus like that, how could Dave have failed to print it?

(UNCLASSIFIED)

To the Editor, CRYPTOLOG:

The [redacted] interview in the December issue of CRYPTOLOG is outstanding! I also think that the interview idea is a brilliant one. There are undoubtedly more than a few of our people at various levels of the management chain and also more than a few of the stalwart experts who would be amenable to sharing their views, experiences, and expertise in this format. The [redacted] interview provided an insight into a story that may never have seen the light of day had it not been for CRYPTOLOG. Truly, SIGINT journalism at its finest!

I am in the process of collecting information for a couple of articles which I promised you some time ago. I hope to surprise you one day and even complete them.

Keep up the outstanding work!

[redacted] G95

Editor's reply

Thanks for the kind words. We're glad you like the interview format, and we hope to use it again soon. Someone else who liked the [redacted] interview, as well as the Kathy Bjorklund article on the SR test, was [redacted] of the SR Career Panel. He requested 50 extra copies of the December issue and intends to give them to current and future SR interns for "mandatory reading" of both items.

(UNCLASSIFIED)

To the Editor, CRYPTOLOG:

In response to [redacted] article "Let's Give Linguists a Bigger Piece of the Pie!" (CRYPTOLOG, December 1976), I say, "No more pie 'til you eat your spinach!"

[redacted] article states or implies the following suggestions:

(a) some sort of quota system should be implemented that would allow the distribution of GG 15-18 personnel in this agency to include *x* desk linguists;

(b) various levels of agency management are unaware of the problem as perceived by [redacted]

(c) an advanced degree in language is *prima facie* evidence that we can expect superior performance as an operational linguist;

(d) we are grossly overpaying linguists at the lower end of the GG scale, while grossly underpaying them at the high end.

Well, sir, that is a most extraordinary group of suggestions, and a group that I mostly disagree with. Let me start at the beginning:

(a) I expect that [redacted] meant to imply some degree of quality in recommending that the desk linguist be included in the 15-18 category. But does he really expect that someone in this agency can or will come up with language analyst billets in that grade range? I don't think so. And I think the rationale behind such a decision would be that "he isn't likely to be worth that much money." Now that's a hard cold look at it, but it's probably closer to the truth than any COSC manual that allows 9-18 as the path of the language analyst. Since [redacted] did not indicate that he was discussing multi-linguists or multi-skilled people, I am assuming that he is including the highly qualified, single-foreign-language, certified language or voice language analyst in his numbers. If he honestly believes that such an analyst is going to make it beyond 12 or 13 without demonstrating a skill beyond turning foreign sounds or words into English sounds or words, using a skill in a single foreign language -- well, I just don't know what measure he is using. P.L. 86-36

(b) A few years ago I would have agreed that the upper levels of agency management were at best unreceptive to the idea of promoting linguists. I no longer believe that. I have seen too many promotions in the last couple of years to the 12-15 range and, while I am certain that there are individual cases of inequity, I would strongly disagree that there are any grounds for a "class action." Our activist language panel would no doubt be offended by the suggestion that it did not know what was going on in the language world. Perhaps [redacted] is not aware that current hiring plans for new agency personnel are almost totally devoted to the acquisition of language technicians.

(c) The issue of advanced degrees in language, I think, has been largely resolved by several developments: a general lack of availability brought about by an overall reduction of language majors at many universities; a requirement to retrain language majors in real-world applications of the language they studied in the academic world -- and all too frequently this training has been at the very basic level, hence expensive; and, last but not least, the "average grade structure" problem which says that we got to hire more people at lower grades, do less promoting above grade 12, and, perhaps most important, keep the language analyst in that job -- the job on which his paycheck is quite likely to depend. Again, I realize that it sounds harsh, but the times are changing. While the agency might like to help the language analyst to move into a different

field and very often did that in the past, I would expect to see a tightening of the belt as more and more interest is shown in the problems we face. Ironic, isn't it? In the years when those language problems were back-burnered, we always kind of assumed that when the linguist got the spotlight he would just zoom ahead so fast, we wouldn't be able to keep up with him. Now that he is in that spotlight -- and, believe me, he is there -- we are going to see, I expect, more actions similar to the recent personnel decision that dropped the entry level for linguists (and others); higher standards for language professionalization; and tighter controls on the language field in general. FYI, our language-hire program for the next couple of years will probably focus on high-school graduates at grades 2-3.

(d) While I don't have much of a problem finding some underpaid linguists in grades 5-9, I personally am unaware of any who think they are underpaid above those grades. But, here again, we may be discussing two different ideas. [redacted] seems to be suggesting that, as a matter of high agency policy, linguists do not get promoted. I would like to suggest that he look lower. Promotion recommendations come from the divisions and offices and, by and large, they get their recommendations accepted.

One final remark: the linguist who flees the field had better take with him some skills other than language. I don't know many desk analysts, TAs, or CAs who are supergrades. If there is ever to be a group of supergrades in the language field, they will come from the ranks of multi-linguists, linguist/analyst/managers, or other multi-skilled people. And that's the truth.

Dan Buckley,
B Language Coordinator
(UNCLASSIFIED)

SPANAKOPITA*

10 sheets phyllo (12 x 15 inches)
½ cup butter, melted
2 packages (10 ounces each) fresh spinach
1 tablespoon salt
2 eggs
2 cups cottage cheese (small curd)
1 cup grated feta cheese
3 tablespoons parsley
2 green onions with tops, minced
Salt and pepper

Cut phyllo sheets into halves and place 10 pieces in a buttered pan (7 x 11 inches). Brush each sheet of phyllo with melted butter.

Wash spinach and remove stems. Cut leaves into ½-inch lengths. Sprinkle with salt and let stand for 15 minutes. Beat eggs. Add cheeses, parsley, and onion. Squeeze liquid from spinach. Fold spinach into egg mixture. Season with salt and pepper to taste. Spread mixture over phyllo sheets in pan and top with remaining 10 pieces of phyllo, brushing each sheet with remaining melted butter. Bake in preheated moderate oven (350°F.) for 40 minutes. Cut into squares and serve hot. Makes 6 servings.

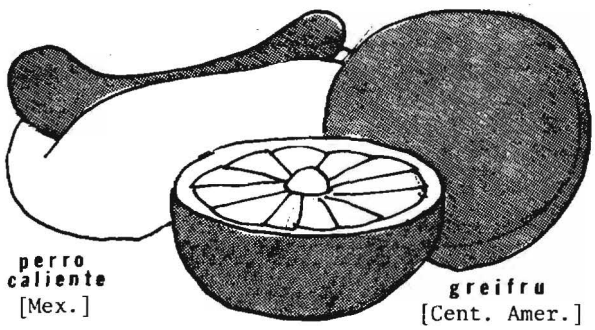
*Greek spinach pie.

SOLUTION TO NSA-CROSTIC No. 6
(January-February 1977)

[redacted] "Anglicisms in Puerto Rico" P.L. 86-36

(NSA Technical Journal, Vol. XVII, No. 1, Winter 1972; reprinted in *NSA Technical Journal: Special Linguistics Issue III, 1976-1978)*

"A linguistic 'laissez-faire' has existed [in Puerto Rico] for a long time. Although schools and newspapers have actively encouraged correct use of Spanish. . ., only the most undesirable borrowings [from English] have disappeared, and . . . new ones have appeared."



perro caliente [Mex.]

greifru [Cent. Amer.]

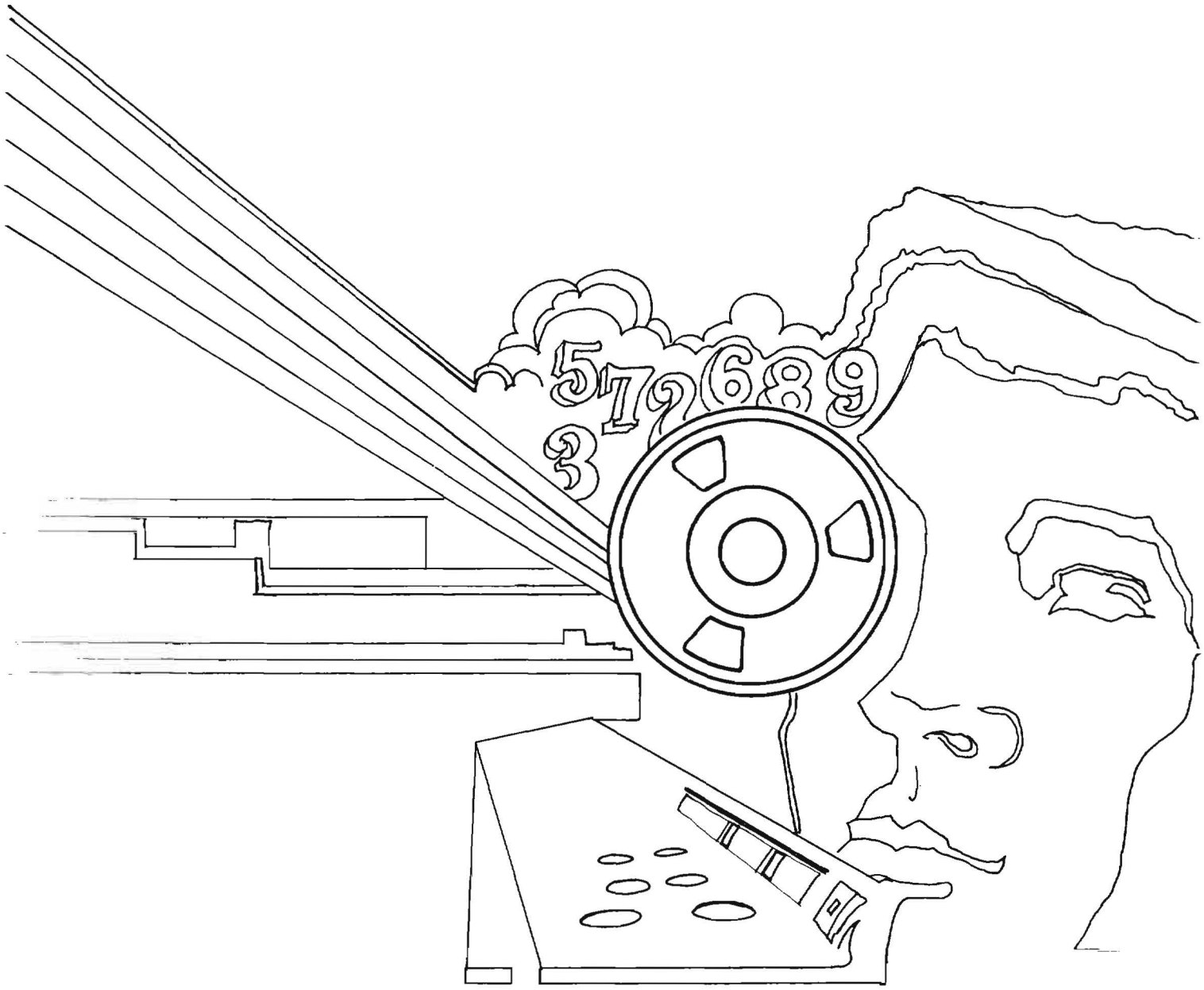
(UNCLASSIFIED)

If you're planning to enter this year's CMI or CLA Essay Contest, or the newly established IAI Essay Contest, you'd better get a move on! The deadline for the CLA Essay is/was 4 March 1977, and for the CMI and IAI Essay Contests is 25 March 1977.

Complete information about all three contests can be found in the Fall 1976 issue of the *NSA Technical Journal.*

(UNCLASSIFIED)

P1-Jan 77-S32-25100


5 7 2 6 8 9
3