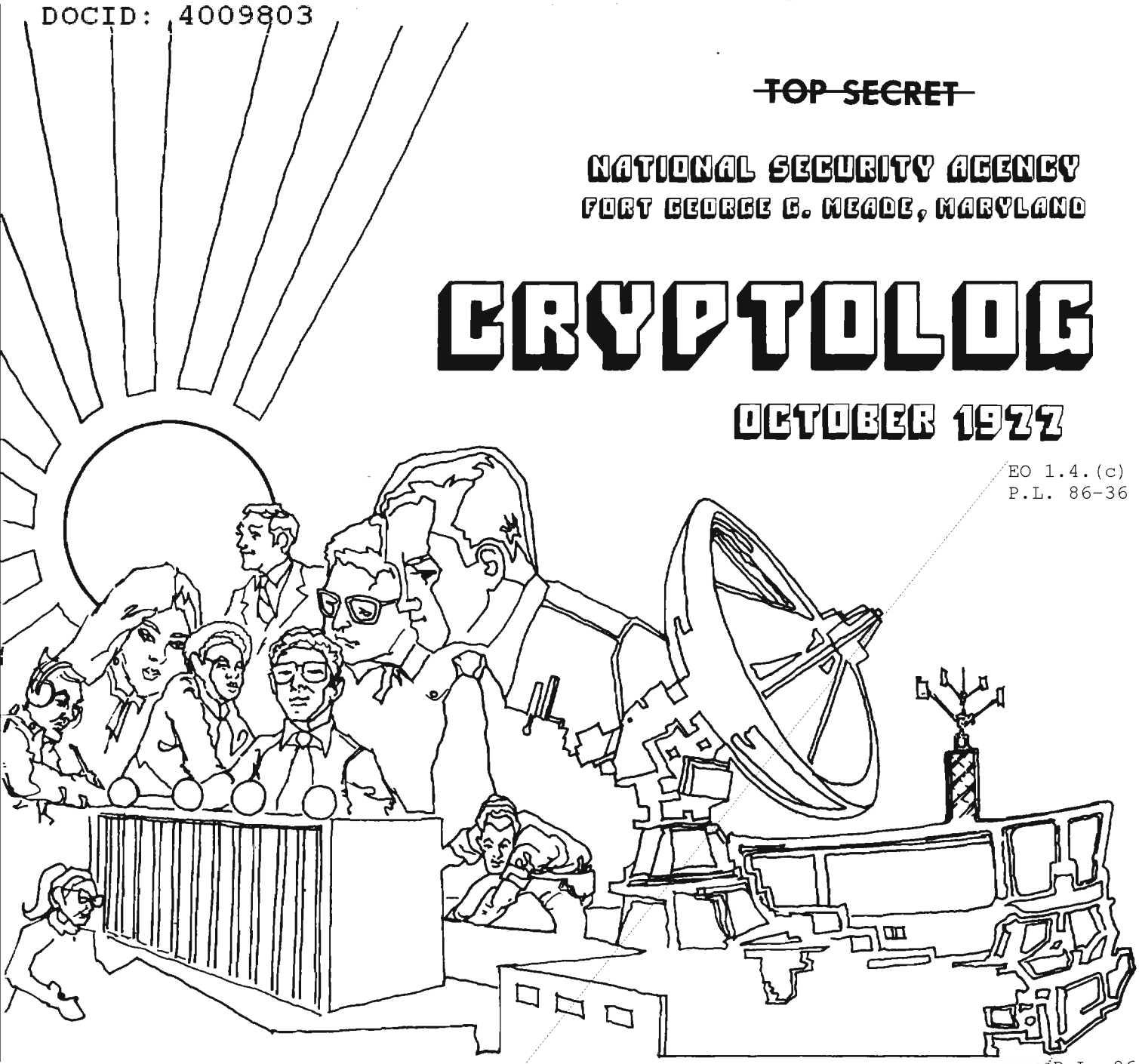
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

OCTOBER 1977



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

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

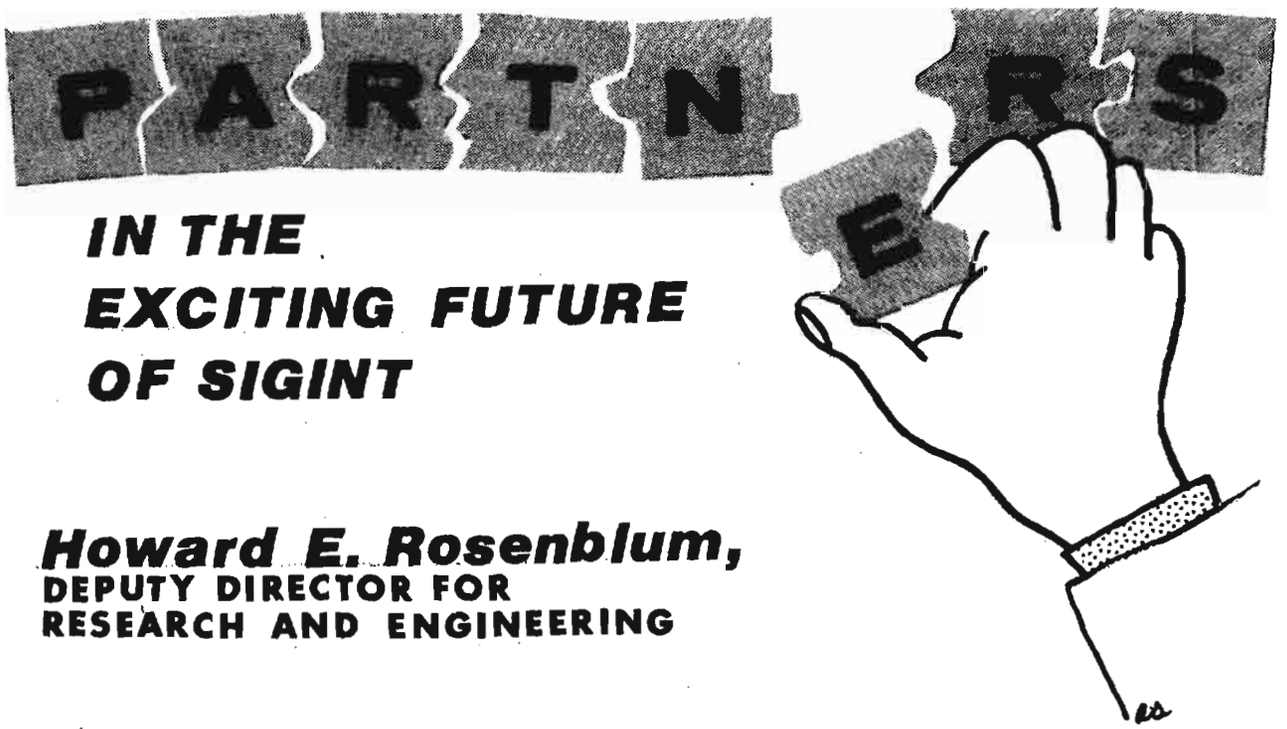
CRYPTOLOG

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

VOL. IV, No. 10 OCTOBER 1977

PUBLISHER WILLIAM LUTWINIAK

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



IN THE EXCITING FUTURE OF SIGINT

Howard E. Rosenblum,
DEPUTY DIRECTOR FOR RESEARCH AND ENGINEERING

Mr. Howard E. Rosenblum, Deputy Director for Research and Engineering, was the guest speaker at the April 1977 graduation ceremony for the National Senior Cryptologic Course CY-600. We considered his perceptive remarks to be of value for a much wider audience than the graduating class and asked Mr. Rosenblum for permission to publish them in CRYPTOLOG. He has kindly granted that permission, and we are now pleased to publish his talk, in a form slightly abbreviated and modified for written rather than spoken presentation.

Ed.

Distinguished guests and members of the CY-600 graduation class: I am delighted to represent Mr. Buffham, our Deputy Director, and address you at the conclusion of your 7 weeks in CY-600. I trust this course has been stimulating, that it has demonstrated the complexities of the SIGINT business, and that it related SIGINT to the Intelligence Community.

Before we get to the graduation ceremony itself, I would like to spend a few minutes with you sharing CY-600 experience and seeking some perspective. You see, I'm a graduate of CY-600 too. I attended the first course given, a pilot course, more than 10 years ago.

I have studied the current CY-600 schedule and I can see that you have covered a lot of ground. You have received tutorial background on SIGINT disciplines, presentations on NSA management, and background on the Intelligence Community. You have seen SIGINT product worldwide. You have toured CIA, NPIC, and even NSA. You have had seminars with NSA seniors and with Intelligence Community seniors. You have had slick "best of all possible worlds" types of presentations, and also some incomplete ramblings that left you uneasy and unsatisfied. You have tried to sift both types, to locate their warts and dimples. It has surely been a broad-based, mind-boggling (and spine-boggling) experience! I have also examined your roster and I see that CY-600 attendance is also broad-based. About 50 percent of you are from non-NSA organizations.

How was my CY-600 course of 10 years ago? I'll cite only the major differences. I am impressed by these differences because I believe that the differences between the first CY-600 course and the current course reflect a change in the National Security Agency and a change in the Intelligence Community, and those changes attest to the responsible maturing of both.

Comparing this course with the pilot course of 10 years ago, we see that that first course had:

- a makeshift, crowded facility,
- an all-NSA student body,
- no speakers from CIA,
- no speakers from DIA,
- no tour of CIA,
- no speakers from the Intelligence Community staff,
- no tour of NPIC,
- no seminar with DIRNSA,
- no seminar with seniors outside of NSA,
- no inputs on military support.

It's obvious that the course has come a long way!

What perspective can one gain by examining the differences between the first and the current course? The differences are not accidental: The CY-600 course has evolved under pressure from its managerial environment. NSA has become less parochial. It recognizes a "community," the Intelligence Community, and the need to be a cooperative contributing member of it. On its part, the Intelligence Community also has become less parochial: it sends students to CY-600 and participates in course presentations. The Intelligence Community thus recognizes a need to understand and cooperate with NSA. NSA and the Community recognize the need for its new wave of leaders not just to be *aware of*, but also to be a *part of* a cooperative, interactive Intelligence Community.

This is what is happening now! The Intelligence Community is slowly growing together. NSA/CSS is a real factor now. Support to military commanders has a genuine thrust. SIGINT is having an impact on tactics. There is less parochialism: "mine" is stressed less and less often, and "ours" is stressed more and more. More and more frequently, tough decisions are being made with a consideration of overall intelligence needs, rather than narrow element needs. CIA, DIA, and NSA actually talk to one another! Cooperative endeavors are under way, with joint review of research and development programs and joint projects. [redacted] The Intelligence Community structure has become ecumenical, with broad Community participation and impact.

So it *is* happening, and the changes I have noted in CY-600 are *not* accidental. The perspective of the course, its objective, is *community*. NSA and the Intelligence Community recognize and depend on each other. All of you graduates of this course -- whether students from NSA, or students from the Service Cryptologic Agencies, CIA, DIA, FBI, DOD, or the military departments -- had a two-fold purpose in participating in it: the purpose of educating yourselves as individuals, and also the purpose of building *Community teams*. As all of you got to know one another during these 7 weeks, you have learned that you are *partners*. Yes, we are all partners in our Intelligence Community future. And what a future we face together!

"May you live in exciting times!" I am told that that expression was a curse in old China, where change and excitement were to be feared. I am also told that in Turkey the same expression was a toast, a challenge given in confidence that change meant opportunity for those with ability. The Intelligence Community is living in exciting times. The world -- the balance of power -- is changing at a bewildering pace. The gathering, reporting, and use of intelligence are taking on critical importance. The Intelligence Community, using American technology, has some amazing tools: satellites for photography, for surveillance, and for communications and control; computers for selection, analysis, editing, and reporting; and technology for [redacted] intercept and analysis. We use the leading edge of semiconductor technology, cryogenics, optics, computing. . . What an exciting array!

And we have a new President, who wants to reorganize. We have a new SECDEF, who wants to reorganize. We have a new ASD C^3I, and a new DDR&E. We have more publicity, and also more controls on us. We have more requirements and fewer resources. These are exciting times indeed, with many changes, with problems and opportunities for all of us. So "live in exciting times!" and make full use of the knowledge that the National Senior Cryptologic Course has given you.

A few weeks ago I had the privilege of attending the swearing-in ceremony for the new Director of Central Intelligence. President Carter was there and addressed the group. Let me paraphrase some of his remarks. The President observed that he had been told of the Intelligence Community, but this was his first opportunity to understand its complexity. (He had just met and spoken individually with the dozen or so heads of the Community components.) He commented on how difficult it must be to ensure that such a complex is coordinated, responsive, and correct. By the way, President Carter said that he expected mistakes, just as he would make mistakes as a new President, but he stressed that they not be concealed mistakes. The President described the Intelligence Community as "damaged" -- damaged by hiding mistakes, by Watergate, by adverse publicity. He resolved to undo the damage. He said he needed good intelligence and wanted to help the Intelligence Community restore its self-confidence and, just as important, restore the confidence of the people of the United States in a Community of needed, professional, productive experts.

So intelligence -- your product, our product -- is needed at the highest level, and that need is recognized by the President, the Cabinet, economic and military planners, and military commanders. Intelligence contributes to arms limitations agreements; formulation of foreign policy; Government options early in a situation; force-structure decisions; warning; tactics and strategy development; countermeasures development; and military decisions during conflict. This range of intelligence has gotten more important to our country as our country has gotten weaker with respect to the rest of the world. Our job is to get intelligence, to protect our means and sources of getting it, and to secure our communications that carry it. And we must do it openly. We must make as much information as possible available to the news media, because our open society so dictates, and we must conduct intelligence operations on American principles, hence more open to the public than intelligence activities of other nations, yet closed enough to protect sources and methods. This process arouses wonder in our foreign

associates as to our openness, and arouses concern among some Americans that we still must keep some information secret.

This, then, is the challenge: Make the complex Intelligence Community work. Make it efficient. Make it responsive. Make it accurate. Keep it clean and open. We must work as a team to make this happen. CY-600 today is designed to help. My CY-600 of yesterday was not.

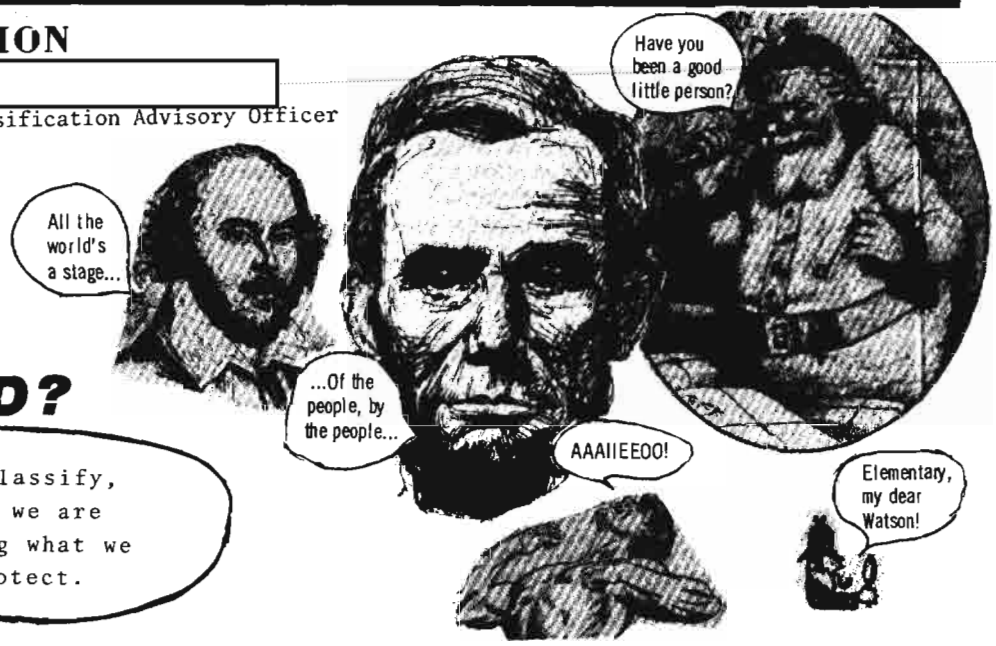
The work that goes on at NSA and throughout the Cryptologic Community is important. It reflects the technical and intellectual talents of many people. It reflects our need to function in an open society. It also reflects the courage and integrity expected of professionals in the intelligence business. The things we are doing in the future will provide American policy-makers and military commanders with critical information and reasoned assessments about the complex foreign political, economic, and military challenges to our national security and welfare. The output from our Agency, our Community, is designed to achieve and to live in peace, rather than only to protect us in time of war. What we do has become an important and permanent element of our national foreign policy and military structure.

~~(S - CCO)~~

CLASSIFICATION CORNER

By [redacted]
DDO Classification Advisory Officer

P.L. 86-36



WHO SAID?

"The less we classify, the better off we are in protecting what we have to protect."

The person who said this also believes that too much secrecy makes it harder to keep the significant secrets. This thought should be well taken by those in NSA who classify papers they originate. The problem of overclassification is real. Although the originator feels safe when he affixes a SECRET stamp on a memo that really needs only CONFIDENTIAL protection, he is only compounding a problem situation that has existed here for a long time.

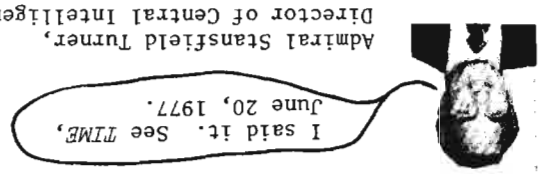
Here's a test for you. Go to a file cabinet in your work area and check the classification of the first ten folders you see. I did, and these were the results:

SECRET - CCO	6
SECRET	1
CONFIDENTIAL - CCO	2
UNCLASSIFIED	1

The higher classification wins every time.

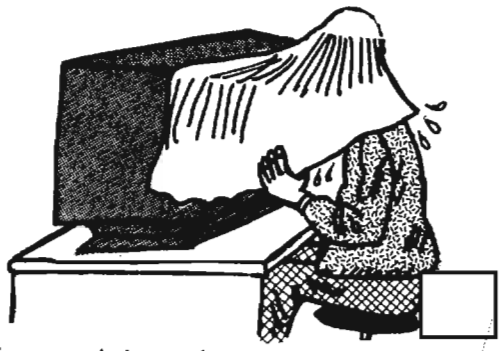
When assigning a classification to a paper that you have originated, remember that DoD Directive 5200.IR, the NSA Classification Manual, and USSID 525 all state that, when doubt exists as to what level of classification is appropriate, or as to whether certain information should be classified at all, the resolution should favor the less restrictive treatment. That is, if you have to choose between SECRET and CONFIDENTIAL, choose CONFIDENTIAL. And if you have to choose betwen CONFIDENTIAL and UNCLASSIFIED, choose UNCLASSIFIED.

Answer:



(U)

HUMAN FACTORS IN THE USE OF MICROFICHE READERS AT N.S.A.



Don Snow, V1
DDO Micrographics Coordinator

The success of an applied micrographics program depends on its acceptance by the user. That acceptance may be slow or fast, and there are a number of factors which will influence it. But one very important factor -- the "user" or "human" factor -- has received scant attention until recently.

The June 1977 issue of CRYPTOLOG began with an excellent article by [redacted] on "Human Factors and Systems Design." Although he was not specific about what kind of system design or designs might be under consideration, Doug seemed to be talking about electronic data-handling systems involving, say, terminals in an analytic area, which are hooked up to a computer, and operated by the user according to instructions developed for the specific type or model of terminal.

A few days after reading Doug's article, I came across another one in the May/June 1977 issue of the *Journal of Micrographics*. This one, by Dr. Robert M. Landau (a sometime consultant to NSA) is entitled "Microfiche Reader Human Factors." In that very detailed paper, Dr. Landau sets his stage by saying,

> "The subject of human-information system interface has been studied and reported on by thousands of people. The physical, psychological and intellectual interface problems of the three major media: paper (hardcopy), micrographic (viewer screen), and electronic (TV or video screen) have been studied extensively. Almost all of the studies have related to the use of electronic (TV/video) media. Less than 100 studies have been directed to the micrographic medium; only a small number of those have been directed to the specific human factors involved in microfiche readers. . ."

That is true, at least in the formal, documented sense. However, we at NSA and our counterparts in the Intelligence Community who are involved in designing and applying micrographic systems have almost automatically included "human factors" in those applications. The reason is simple: we wanted the application to succeed. And it would really succeed only if the user or users accepted it.

Many of the factors discussed below are included in Dr. Landau's article. The main difference lies in the fact that he was addressing a readership comprising *makers* as well as users; and, among the users, people in the world of business and commerce as well as government. My article is aimed at those readers of CRYPTOLOG who are, or may become, users of microfiche and microfiche readers.

P.L. 86-36

FICHE-RELATED FACTORS

Film thickness

First-generation (i.e., "master" or "from the camera") silver halide film is usually 4 mil or 5 mil thick (.004" or .005"), regardless of whether it came from a source-document camera or from a computer-output-microfilm (COM) camera. If additional copies are required from that "master," diazo film stock is used. Diazo microfiche are 7 mil (0.007") thick, making them a bit stiffer and more durable than the silver halide "master." It is important to note that smudges or fingerprints on silver film are permanent, while such blemishes can be carefully wiped from the surface of diazo film. For that reason we always recommend that first-generation silver halide film be used as "record" or "later duplication" copy, and diazo duplicates be used as "working" copies.

Polarity

First-generation film comes from the camera in the *negative* mode -- clear characters on a dark background. Diazo duplicates retain that negative polarity; this is another "human factor" we use here. It creates far less eyestrain to look at a page of information on a reader screen if the characters are clear and the rest of the "page area" is dark, than vice versa. Admittedly, the user must become accustomed to that switch; for example, right now, you're reading this article as black words on a white page, which most hardcopy readers are used to. But the frequent user of microfiche soon appreciates the negative polarity when looking at a reader screen.

PHYSICAL CHARACTERISTICS OF READER

Controls (type and position)

This is not much of a problem at NSA, since we have standardized on one or two types of fiche readers. Remember, this article is limited to fiche readers and does not address the area of reader/printers. For the most part, at NSA we see a considerable number of W.S.I.

(Washington Scientific Industries, Inc.) Mini-Cat Model 1114D readers (Fig. 1). (The model

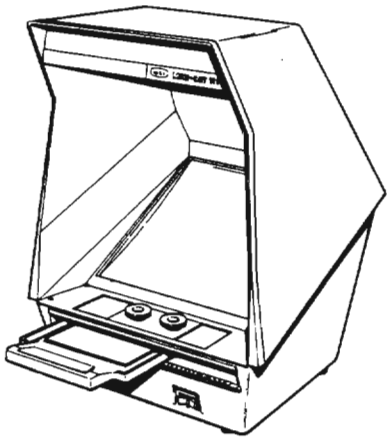


Fig. 1

number reflects the dimensions of the screen -- 11" high by 14" wide, and the "D" indicates dual lenses.) These models are hooded, with a front-projection system reflecting the image onto a screen tilted about 60° from the vertical. (That feature is a boon to people with bifocal glasses -- still another "human factor" of importance to at least *some* of us!) The fiche carrier is free-floating under the lens in use; it moves in the *opposite* direction from the sequence of pages on the fiche. Column coordinates are etched on the front edge of the carrier traverse area, and row coordinates are etched on the left and right edges of the carrier itself.

The other model is made by Realist Inc., in their VANTAGE line (Fig. 2); depending on how long or short a time the user has had it, it could be a Model I, II, X-II, COM-IV, or IV. They have the following features in common: rear projection onto a vertical screen; a free-floating carrier with a pointer attached to it (the pointer points to the particular grid area, on a

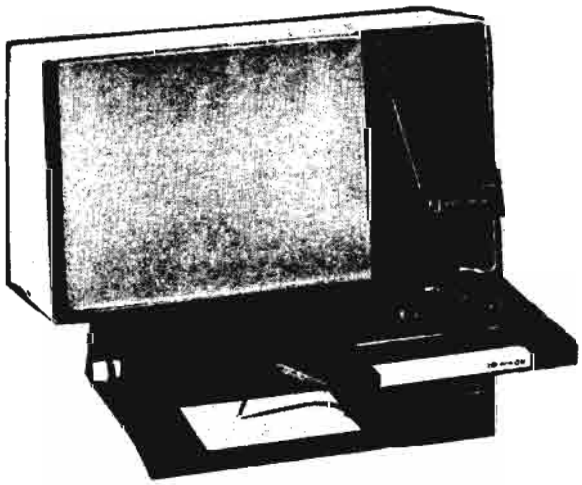


Fig. 2

fiche-size printed card, which is being projected onto the screen). The carrier moves in the *same* direction as the sequence of pages. By moving the rear of the reader body in and out, the user can increase the magnification of the lens used by as much as 25 percent, thus projecting a portion of a page in larger-than-original size.

Fiche insertion and removal

To the novice, this is always a problem. With all the fiche readers on the market, each having its own "special" optics system, the beginning user is not sure how to insert the microfiche into the carrier. Fortunately for us, the problem has been resolved. In the W.S.I. Mini-Cat model, the fiche is inserted into the carrier with the title area *face up* and toward the user. In the VANTAGE line, the fiche is inserted with the title area *face down* and toward the user. There are decals (Fig. 3) which can be applied to the

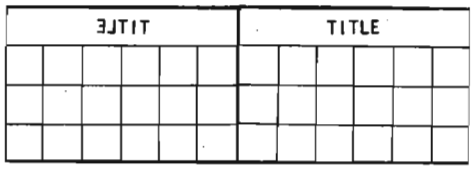


Fig. 3

carrier frame of each model, to serve as a guide for the proper insertion of the fiche the first time. *One reminder:* When placing the fiche between the glass plates of the carrier, be sure that you put it as far *right* and as far *away* from you as the carrier will accept. That will ensure that the grid coordinates will give you the desired page image. (Another "human factor" suggestion!)

Screen hood

As noted earlier, the Mini-Cat has a hood as part of its design. The VANTAGE series of models, however, have a front-mounted vertical screen. If your work area has windows, the placement of your reader is important because of ambient light. The screen should *not* face a window area; if it did, the brightness of the image on the screen would be considerably lowered by the light coming in through we window. (We have found this to be particularly true during daytime hours; moonlight doesn't seem to have nearly so much effect on screen luminance.)

If you want to maintain the brightness of the image on a VANTAGE reader, either sit so that *you* face the window, or tape a cardboard hood around the top and sides of your reader. A hood of about 4 inches should cut off most ambient light.

Screen size

Both the Mini-Cat and the VANTAGE lines have screens that are horizontally oriented. As noted earlier, the dimensions of the Mini-Cat screen are 11" high by 14" wide (the dimen-

sions of a regular computer print-out page). Those of the VANTAGE line are 10" high by 14" wide; however, the optics system will still project a full page-image of computer print-out information. Both models have a thin black reference strip across the middle of the screen.

Size of reader

Both readers discussed in this article are big. This is a "human factor" which the equipment makers are only now beginning to realize. There is practically a void between the bulky, desk-top readers and the "available light" hand-held viewers. The next 3 or 4 years, in my judgment, will see the development of compact, less bulky, and yet high-quality readers. (Admittedly, there are a few "attache case" types of readers on the market, but they're far from perfect, as far as human factors here at NSA are concerned.)

OTHER FACTORS

Reader availability to user

This is a tricky one, since it depends on a number of variables. The following examples are only a few of the variables:

- the number of people in a work area (section or branch), and, among those people, the number who have to refer to material on microfilm;
- the proportion of information on microform to information in hard copy;
- the number of times a day (or week) a person has to refer to microform information.

Ideally (this is currently in effect in some work areas in B Group), each analyst should have his or her own reader. Then the question of availability to the user is answered. Not only is there no competition, but the user does not have to get up and go to the reader -- it's right there on his or her desk.

All is not lost, though, if you don't find yourself in that ideal situation. A good micrographics-system designer should be able to recommend the appropriate number of readers for a work area, after taking into account the variables mentioned above, along with work patterns, schedules, deadlines, and the other things the SIGINT flesh is heir to.

Security

While it is true that information on microfiche is the same as information on hard copy (and thus subject to the same handling and storage precautions), there is one important distinction: the physical dimensions and bulk of a sheet of microfiche are far *less* (by about 98 percent) than the hard-copy version it represents. A few examples: A source-document report of over 90 pages will fit onto a single 4x6" microfiche at a 24X reduction; a computer print-out of 270 pages will also go onto a single microfiche at a 48X reduction.

When a person finishes with that report or that print-out in its hard-copy form, he or she knows that it has to be returned to its proper place in the files. If it were left on top of the desk, it would be very noticeable. Consider, though, the single microfiche version of either of those. The user must put it into a reader, in order to peruse any portion of it. When the user is finished -- *if that user is careful* -- he or she will remove it from the reader and replace it in its proper place in the microfiche files.

To help in this regard, and to make life more pleasant for the user, the Marine guards, and the char force, we have a SECURED card (Fig. 4),

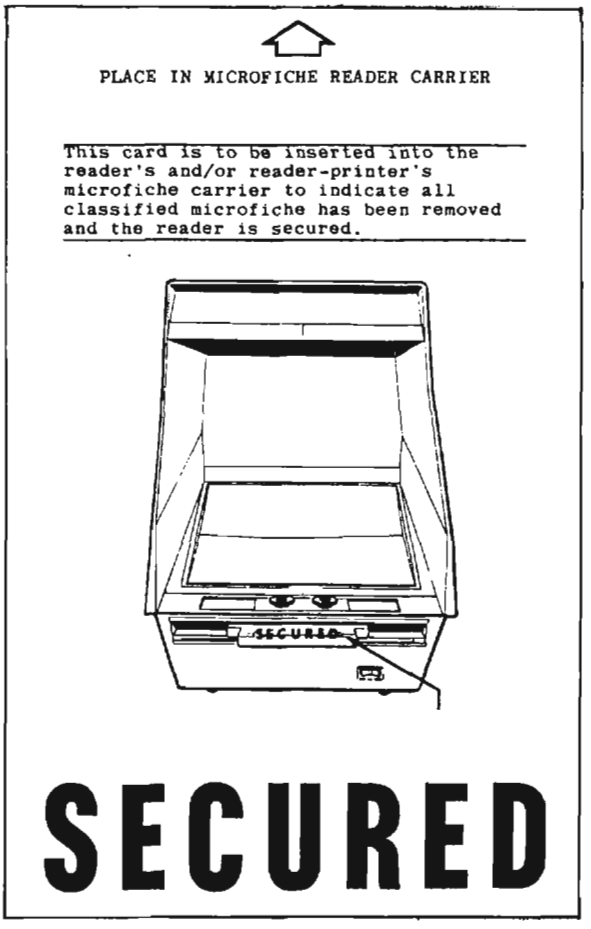


Fig. 4

which fits between the glass plates of the carrier, and indicates that ". . . classified microfiche has been removed and the reader is secured."

Summary

This article has discussed only a few of the "human factors" involved in the acceptance and effective use of microfiche readers. There are many others which -- perhaps together with a discussion of reader/printers -- will be treated in a subsequent article.

Reprints of this article available from Harry Goff, 3W076, 4998(s).

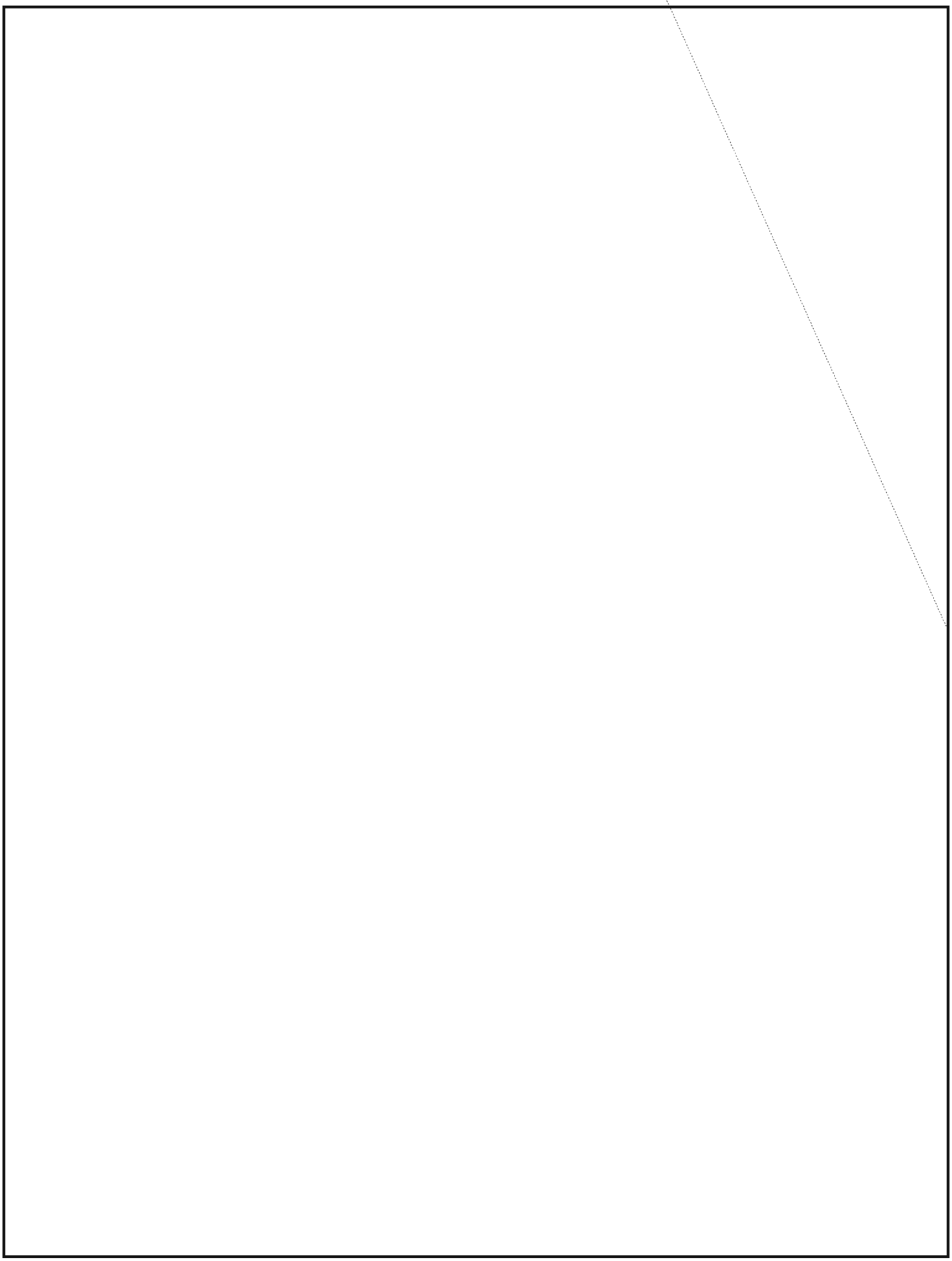
EO 1.4.(c)
P.L. 86-36

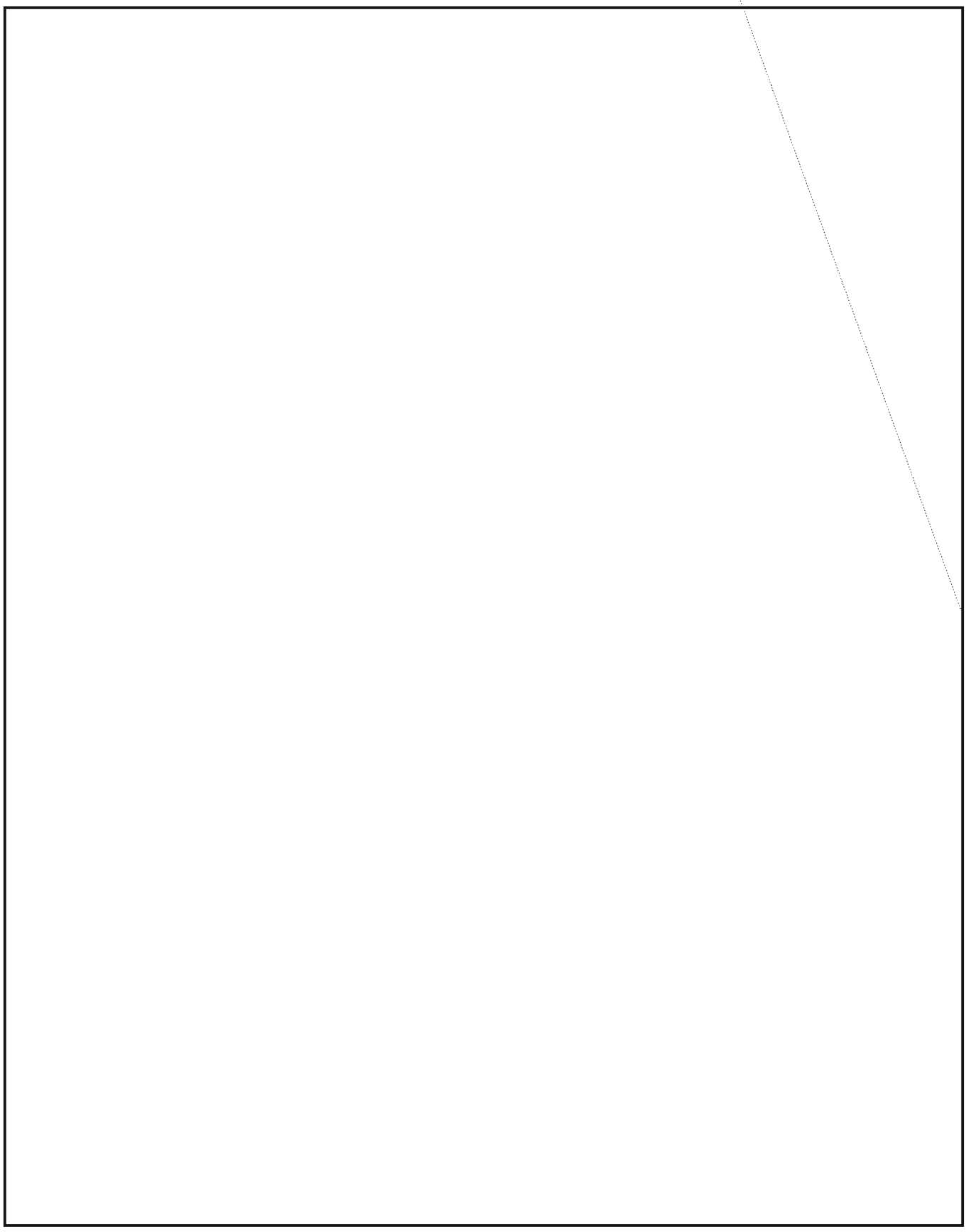
~~SECRET~~

P.L. 86-36

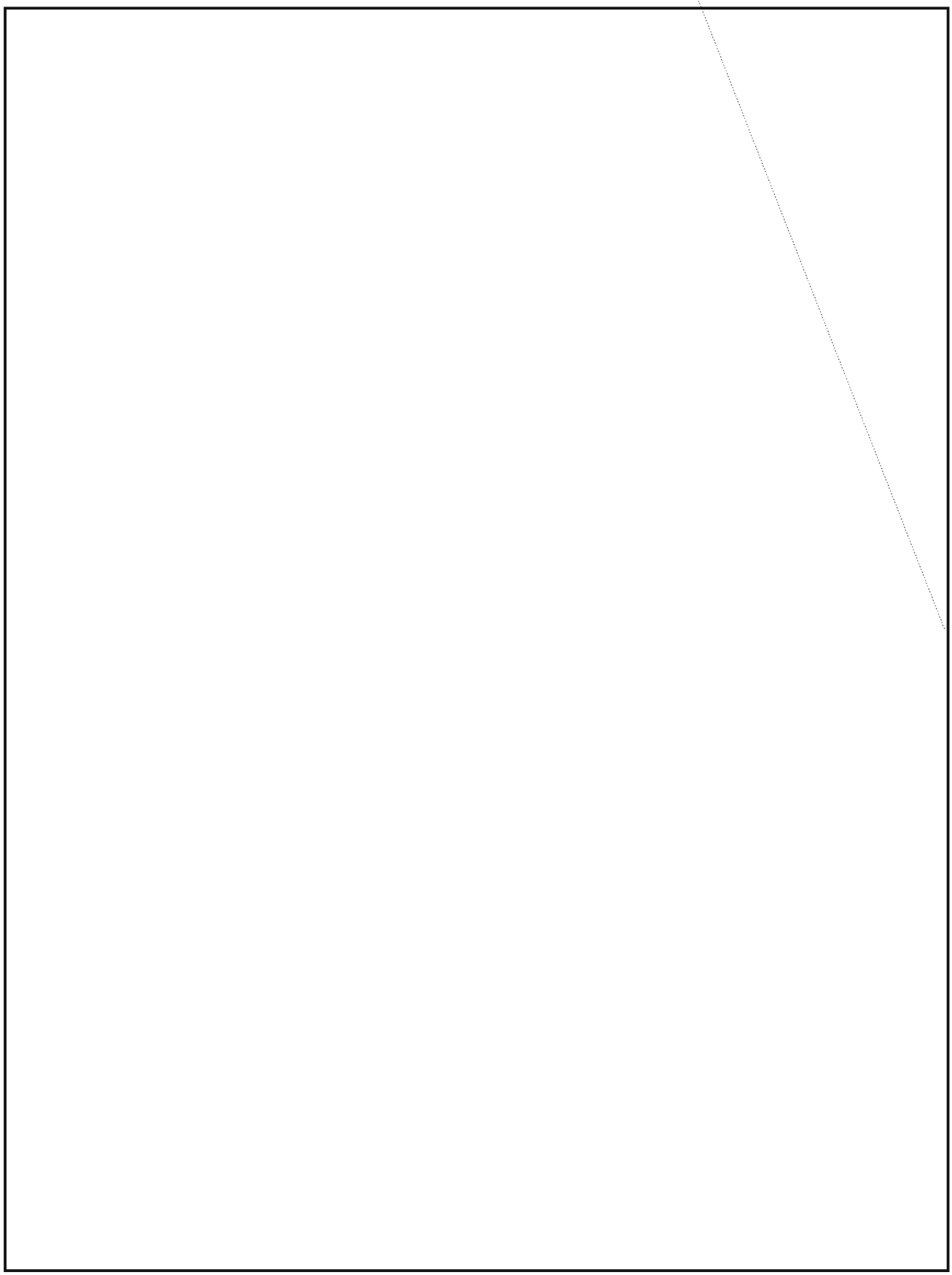
EO 1.4.(c)
EO 1.4.(d)
P.L. 86-36

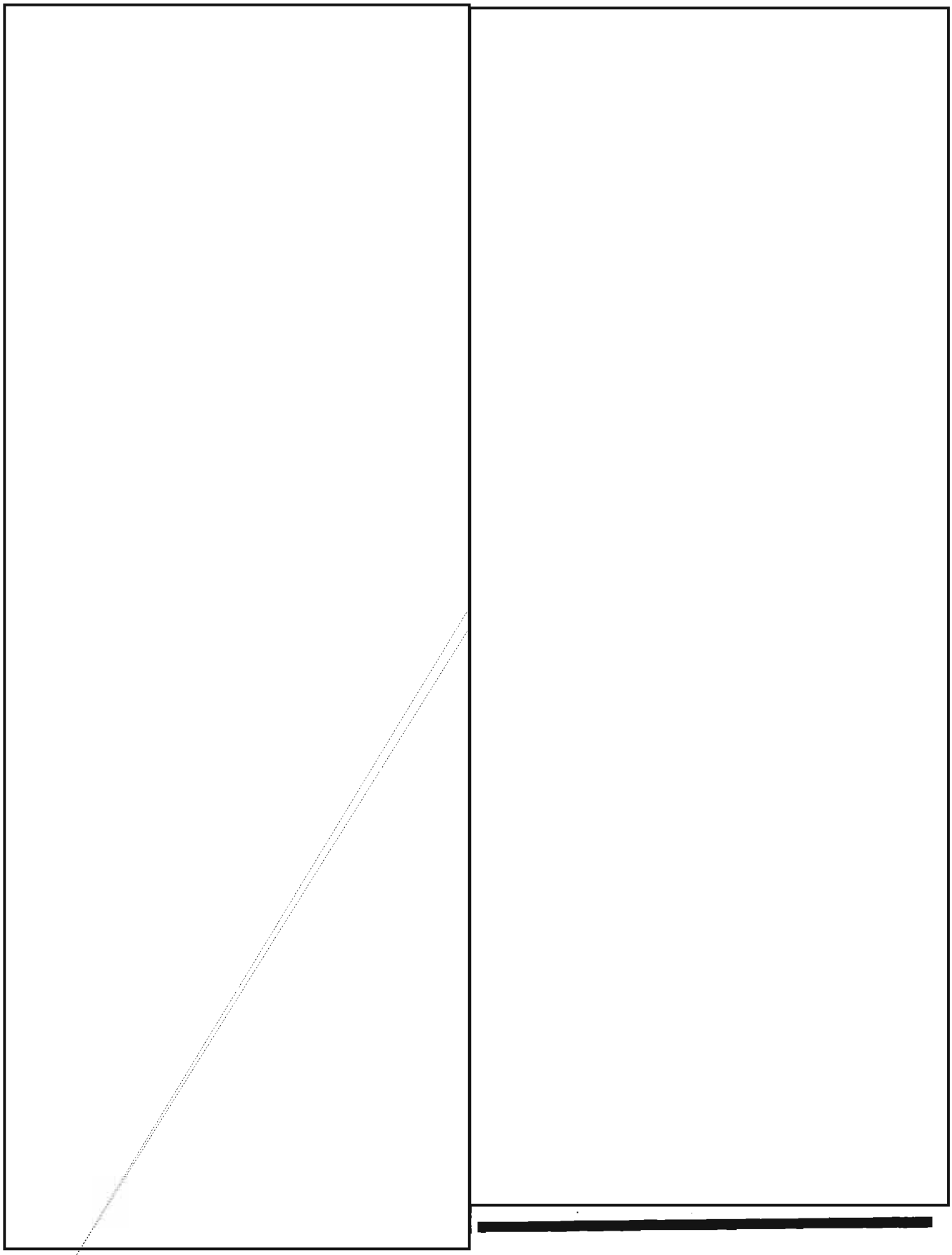
~~SECRET~~





~~SECRET~~





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

WHICH NUMBERING SYSTEM SHOULD WE USE?

By Jess Asken

Interoffice Memorandum (Informal)

Subject: Decisions

Just a quick note to fill you in. I know you're just getting settled in, but some matters are pressing and we need to make some decisions rather quickly. I've taken the liberty of jotting down some questions and "thinking out loud" to give you some background.

We are setting up this communications center and we need to decide now what records should be kept, so that all the instructions can be written out, double-checked, and then issued to all parties concerned. What sort of numbering systems should we use? We need to decide very soon.

First of all, there's the radio station. I think we're going to need the strictest kind of control over messages coming into the station so that nothing gets lost. Radio operators can get so involved with their schedules and frequencies and transmitter adjustments that they forget all about the messages they are supposed to send. (I'm sure the Signal Officer will send down another one of those complicated signal plans he likes so much. He never seems to appreciate simplicity.)

We'll have to decide what system to use. Sometimes the simplest serial system is the best -- like a single log book for every message. Everything gets logged in the same place in the same way. That way, everything coming in gets a number and is controlled. Of course, if there is a lot of traffic, we may have to keep several logs and maybe split the traffic into "up-echelon" and "down-echelon." (Which log should contain the lateral stuff?) I wonder what sort of status reports the Staff will want from us? If they are going to require message volumes by subject matter, maybe we should organize the log books that way -- one log book for each subject. Then all we will need to do to get the volumes is pick off the last number used. Of course, if we get a batch of inexperienced people coming in, they will make a mess out of anything that isn't very simple. What do you think?

Circular messages go to more people, so they are probably subject to more queries -- maybe they should be logged separately. Servicing can get to be a headache whenever we start handling lots of messages. The busier we are, the more errors we'll make. We *could* give each message a unique date and time of file and then only accept servicing queries if they reference the file date and time; but if the messages pile up at certain heavy times of the day (such as at close of business), the file times would get pretty artificial and we wouldn't be able to measure how long it took messages to get out. The alternative is to use a date/time stamp as the message come in and, if two messages come in together and get the same date and time, don't worry about it -- they can be distinguished by their serial numbers. We need to decide which system to use.

Most servicing queries come in because the recipient can't break out the message. Maybe we need a master log in the crypto center so that servicing queries can go right in to the cipher people. I wonder whether we need a master log in the crypto center, or one log for each system. (If we use different logs for different systems, maybe each log should have a unique numbering range, so there could be no confusion about which system/log book was being referred to.)

What do you think about requiring each message writer to use some serial number system, maybe with his own organizational designator as a prefix, on all the *outgoing* messages? Then it would be a lot easier to distribute *incoming* messages that begin with "Reference your number . . ." to the *right* people. (Some people get irritated when they don't get their incoming messages.) Should we set up a standard system or let everybody set up their own?

Whatever we use, I suppose the Signal Staff will insist that all our serial numbers be enciphered. I think we need to fight that, unless they come up with more people for us. Maybe we ought to start a study *now* on the extra work load that would cause us.

We need to develop some thoughts on how often the log books will have to be replaced. If the radio station log books are replaced *daily*, we can get each day's operations reviewed the very next day for whatever corrective action is needed -- that ought to keep them sharp! Of course, the logs in the crypto center ought to stay there for a while, at least until the bulk of the servicing is over. Maybe monthly or yearly.

Maybe what we need is a master log in the message center. . .

CLASSIFICATION: A BIGGER PICTURE

By [redacted] P16

Before one delves into the many specifics present in the subject of classification here at NSA, it might be useful to step back and examine the world of classification in the large. Often because of one's particular job at NSA, or even in the Intelligence Community, this global view of how the various classifications relate to each other is lost in the myriad of detail needed to perform that job adequately.

In so far as the cryptologic community is concerned, the world of classification can be described at its most absolute level by Fig. 1. This diagram takes into account the National Level classification, while also showing *the* three compartments with their interrelationships. The National Level classifications are represented by the area of the rectangle outside the three circles, which themselves represent the individual compartments.

It may be surprising to hear that there are only three compartments. The colloquial use of that word in the shop talk at NSA is often imprecise and leads one to draw erroneous conclusions. A compartment is a special control structure in the Intelligence Community controlled by a National Level agency. Access to the information contained in the compartment requires an oath to abide by its special controls and an indoctrination. Compartments have unique codewords with which to protect the specific information, along with a "channel." This is most notably seen in the "Handle via ---- channels only" and "Appended documents contain codeword material" caveats.

This is as opposed to special access briefings used to control information to very specific

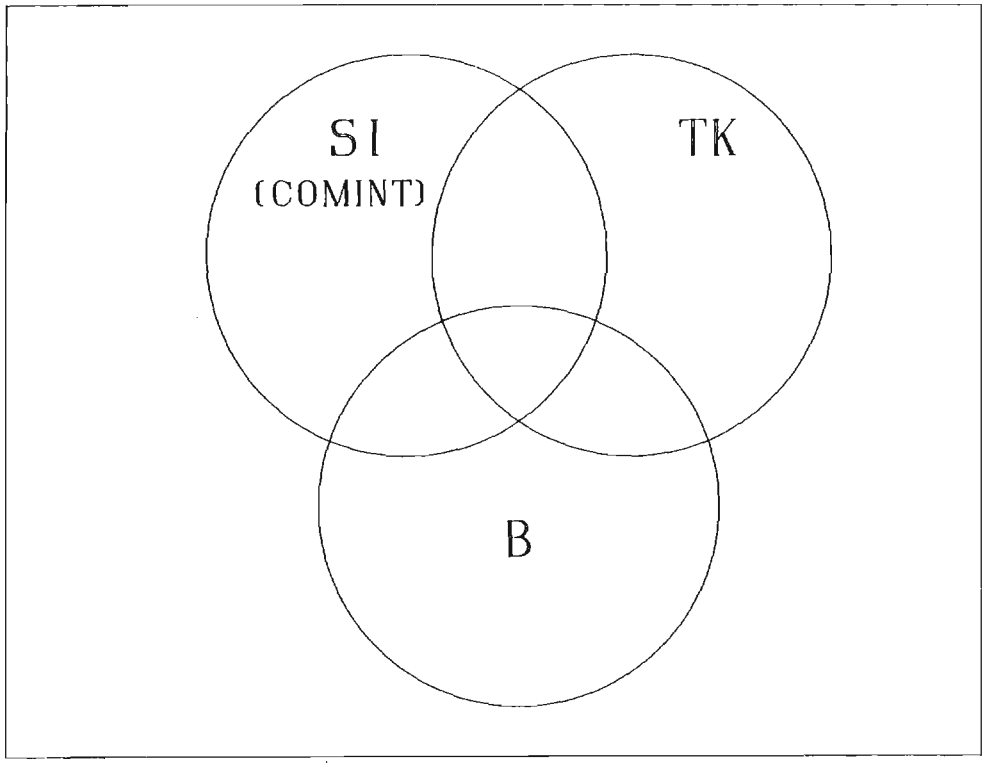


Fig. 1. The Classification World

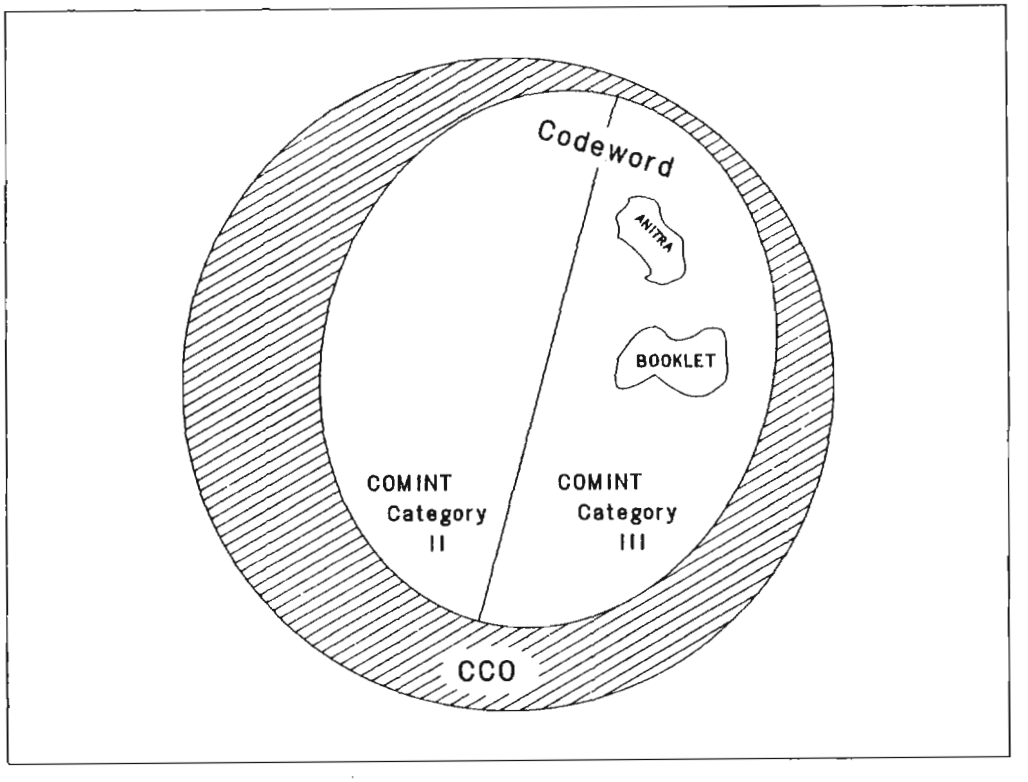


Fig. 2. COMINT Classification

projects, unlike the very broad nature of the information controlled by a compartment. Special access briefings are controlled by the office involved in the project. These accesses do not have codewords but merely append the name of the special access clearance to the appropriate classification following any necessary codewords. Hence we might have a classification "TOP SECRET UMBRA DESKTOP" if there was a project which required access to the material controlled by a special access named DESKTOP.

The three compartments of interest to the cryptologic community are COMINT (referred to as Special Intelligence by those outside this compartment), TK, and B. Each can be easily distinguished by the type of codeword used. COMINT codewords always have five letters (e.g., UMBRA, SPOKE, GLINT): TK codewords have four; and B codewords, six. Each has its own special channel and National-Level OPI. It often happens, however, that some specific project or piece of intelligence falls under more than one of these compartments. For this reason, the circles in Fig. 1 are mutually overlapping. Such a piece of information would have to bear the caveat: "Handle via ----- and ***** channels jointly." The names used for special access, however, follow no similar clear-cut rule and appear to be randomly chosen.

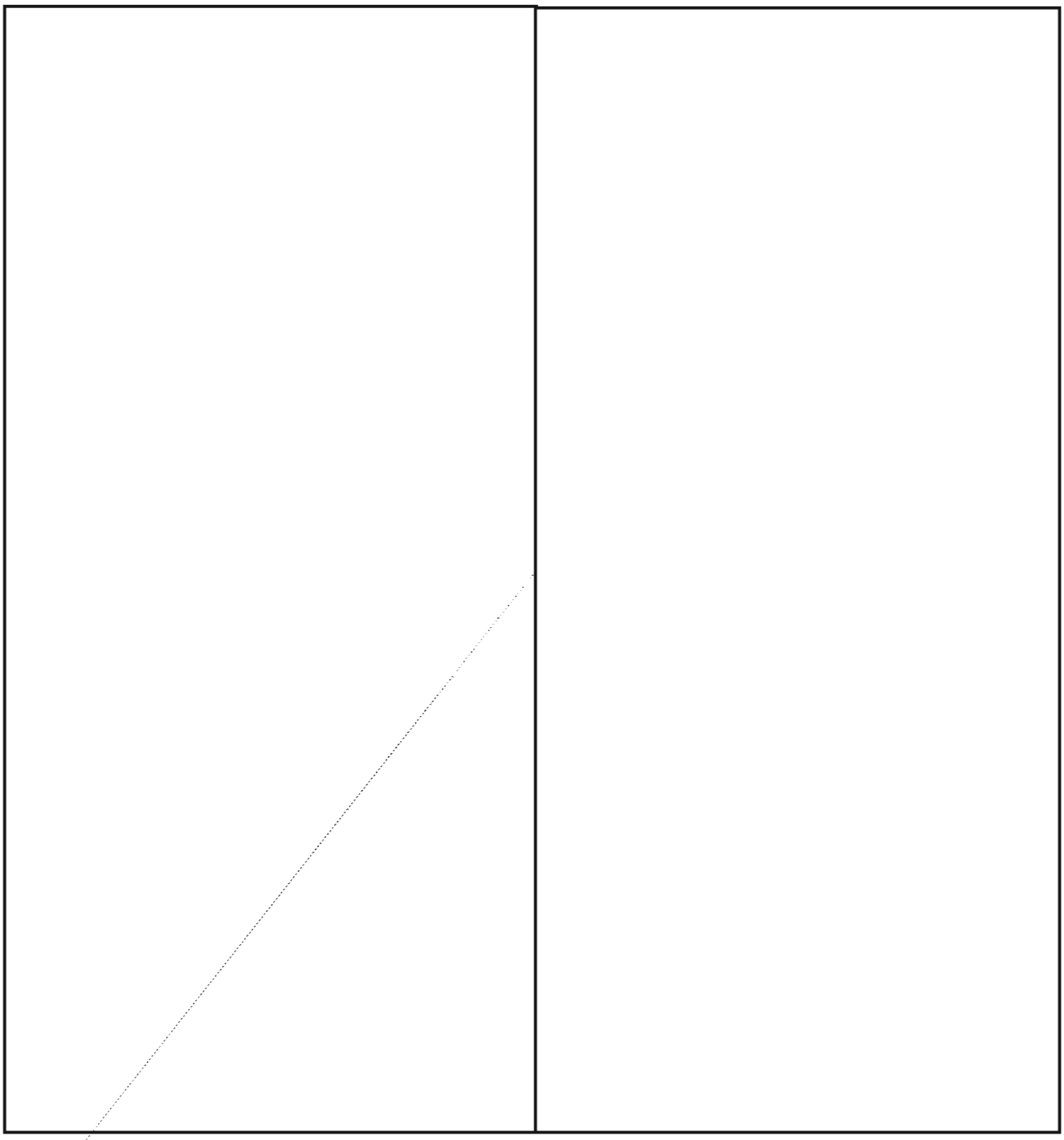
The COMINT compartment also has a substructure. The next level of detail is shown in Fig. 2. Information which falls between the two circles (the shaded region) requires COMINT channel handling but no further protection. More sensitive material is protected by a codeword. Hence "TOP SECRET UMBRA" implies the additional caveat "Handle via COMINT channels only." The classification "TOP SECRET CODEWORD," while in itself not so specific, is, however, used only for COMINT materials. Within the COMINT Category III codeword section are the various special access restructions.

Working at an agency like NSA, where almost all personnel are cleared for access to one of these compartments, one can lose sight of the very restricted nature of the information one has access to. It can be quite a shock to work with other people in the Intelligence Community or the military who are cleared up to the national secret or top secret level but who do not have access to COMINT. This shock strongly reinforces one's appreciation of the sensitivity of the work being carried out at NSA.

~~CONFIDENTIAL~~

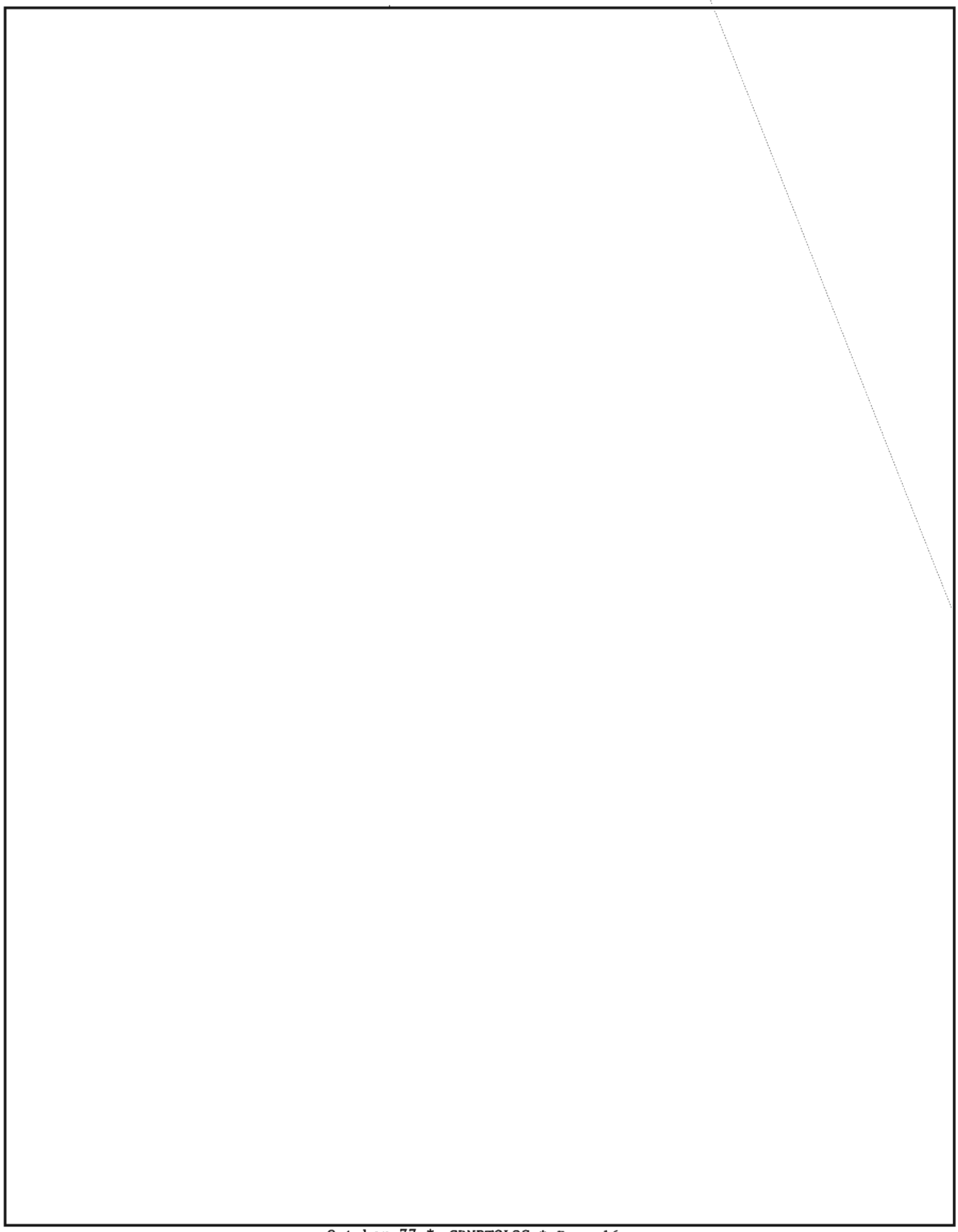
K1- "S.C.A. FIELD MANAGEMENT AND EVALUATION"

K1 P.L. 86-36



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

~~CONFIDENTIAL~~



The Perils of Being a State Department Interpreter

Reprinted from the Department of State Newsletter, June 1977.

On his very first assignment as a State Department interpreter, Theodore E. Herrera faced a most difficult challenge. He was called on to interpret a joke.

The setting was a table for three at an elegant restaurant in New York. Mr. Herrera sat between the rector of a South American university -- a guest of the United States -- and an official of an American foundation engaged in educational projects.

"Now this guy walks into the saloon," the American said, as the interpreter rendered his words into Spanish.

"He says to the bartender, 'Blindfold me and pour me any drink in the house. I'll tell you the brand.'

"So the bartender pours him a few, and each time this guy not only calls out the brand, but he also gives the proof and how old the whiskey is.

"The bartender figures to himself, 'I'll fix this wise guy.' So he pours some water into a shot glass and says, 'O.K. Tell me this one!'

"The guy sips it and lets it go down slowly. He thinks a minute and then he says, 'I don't know the brand, but I'll tell you one thing -- it's never going to sell.'"

The South American had been listening with a polite smile. When the punch line came, he wasn't aware of it. He merely looked on with the same smile and waited patiently for the next sentence -- as silence descended.

"After that," Mr. Herrera recalled in a recent *Department of State Newsletter* interview, "I promised myself I would always give notice to the other party that a joke was on the way. This becomes the cue for a courtesy laugh, at least, and after that, things tend to go very well."

Mr. Herrera is one of 18 full-time interpreters in the Department's Language Services Division. Each of them has to develop techniques for meeting the challenges of their profession whether they are acting as simultaneous interpreters, with earphones, at international conferences; sitting in on important negotiations like the SALT talks; working on the joint Apollo-Soyuz space project with the Soviets; or escorting foreign VIPs on tours of the United States.

Nora M. Lejins has a way of using her eyes to encourage principals to speak to each other, rather than to her. "I was in the Oval Office at the White House once," she related, "interpreting for the President and a high German official. The conversation got very animated.

"Then I noticed that each party, after making his statement, paused to look at me. It got to the point where both of them seemed to be talking to me, as if I were the one who was giving the argument on each side.

"This became disconcerting for me, and I thought it was wrong. I felt they couldn't be communicating very effectively if they spent so much time watching me instead of sizing up each other.

"So as one looked at me, I sort of took hold of his eyes with my eyes and then, by moving my head, led his eyes over to the other principal. Then I did the same thing with the second party when the reply came.

"It worked. After a while, they weren't noticing me any more, and they were speaking directly to each other. I've found it necessary since then to use this technique from time to time."

"It sometimes might look to others like a game of Ping Pong," Mr. Herrera said, "but interpreting is not so simple a matter as an interpreter merely paddling words back and forth.

"Your mind has to do several things all at once while the conversation is going on. You

have to listen and you have to speak, but of course what you say is not what you hear.

"I don't mean just the switch from one language and vocabulary to another, and then the reverse. It's really the ideas that you are trying to communicate, not a word-for-word statement.

"What you have to do is transmit the real meaning in the spirit in which it is being said, and this often means being an actor -- without making it obvious.

"You are handed a script on the spot -- what one of the parties is saying -- and then you have to perform that script, faithfully and convincingly, in the other language.

"I'll give you an example. I was escorting a Latin American official in this country who was invited to address a joint session of a state legislature. He was a very emotional speaker -- an accomplished orator.

"I sensed that I could not do him justice as an interpreter unless I worked myself into his mood. So when he shook his fist, I shook my fist. And it went on like that. I was able to do most of it with intonations and inflections, but I had to use some of his gestures as well.

"When the speech was over, one of the state legislators came up to me and said, 'With a voice like yours, you should be in politics.' I knew then that I had succeeded in putting the principal across, and I felt very good about it."

"All of that is true, but up to a point," said Theodore H. Leon, head of the Language Services Division. "We don't go as far as the interpreter at the United Nations who found his principal pounding the table, so he pounded the table -- and then, when the principal knocked his water glass off the table and smashed it, so did the interpreter.

"I tell our own people, 'Don't go so far as to knock down the glass. If the speaker wants to do it, that's his privilege. But it's not your privilege.'"

Mr. Leon continued, "I can tell you, after 32 years here at State, that this can be a very tricky business. On the one hand, you're supposed to interpret for the speaker by saying only what he says -- without trying to improve on it or knock it down, or otherwise change it.

"If he repeats himself, for instance, then you're supposed to repeat yourself. If he exaggerates, you exaggerate. If he discounts something, then you do so too.

"But, on the other hand, word-for-word interpreting can lead you into a trap, and sometimes you can see it coming, but you might not be quick enough to escape it.

"What comes to mind is an international conference we had once on the spawning grounds of fish. The speaker was British and, speaking an English that was perfectly proper, he said, 'Just put yourself in the mackerel's place. Now what would *you* do if *you* were a mackerel?"

"The interpreter repeated this in French. When he came to the word 'mackerel,' he plunged right ahead. The audience reacted immediately, breaking up with laughter.

"The British speaker was surprised and embarrassed because he had been discoursing with great seriousness and had had no intention of being funny. What he didn't realize, of course, was that mackerel in French has a second meaning -- denoting a very unsavory individual."

Ms. Lejins said, "One way the interpreter could have got around that would have been by saying something like this: 'What would *you* do if *you* were that species of fish?' That would have been neutral. He could have skipped the word 'mackerel.'

"But, while we're on that point, let me say that an interpreter is lucky sometimes if she can keep up with the speaker on a word-for-word basis. Usually we can't. That's why we often have to take notes.

"I was taking notes furiously one time when a West German cabinet minister came here to confer with our Secretary of the Treasury. The German was very, very loquacious, and he had already worn out the German interpreter he had brought with him. That was in the morning, and she asked me to take over in the afternoon.

"The cabinet minister, once he got going, would speak sometimes for 20 minutes without stopping. Now, of course, I'm not a stenotypist, but that's not the kind of skill that was needed in this situation anyway.

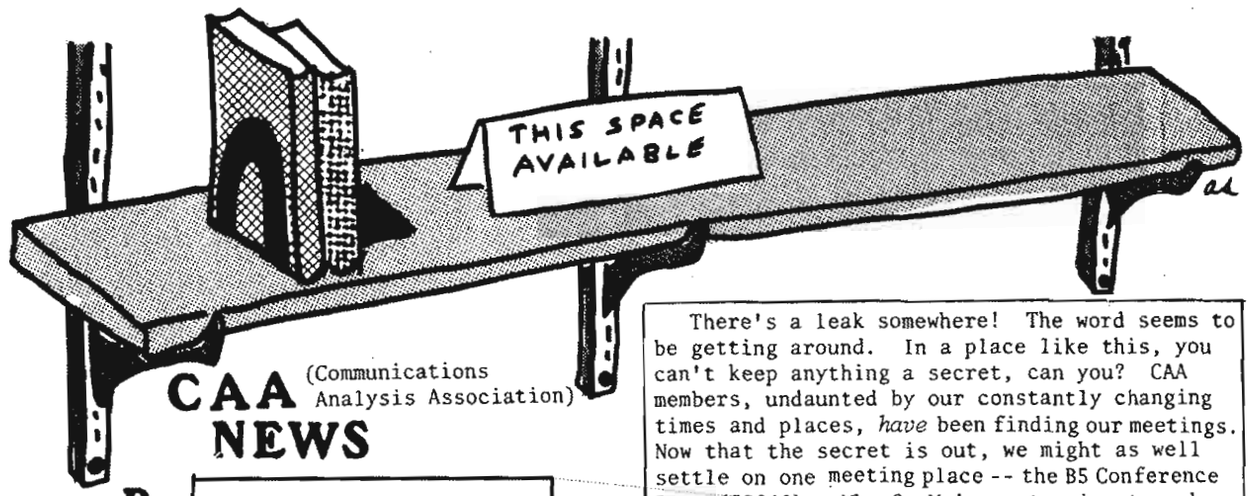
"The idea was to get the sense -- accurately -- of what the cabinet minister was saying and then, when he was finished, to recount it in English.

"The reason for taking notes was to make sure I would leave nothing out. But you can imagine the pressure an interpreter is under in a case like this. If the principal has spoken for 20 minutes, then you also have to speak for 20 minutes when your turn comes.

"It just wouldn't do to abbreviate. You can't take liberties like than when you're interpreting."

(Editor's note: Mr. Herrera was born in New Jersey; his mother had come here from Spain and his father from Puerto Rico. Ms. Lejins was born in Germany and came here as a child; she majored in the Romance languages in school but also studied German. Mr. Leon was born in West Virginia; his first "and most difficult job," he says, was teaching freshman English to American college students; he came to the Department as a translator.)

~~CONFIDENTIAL~~



CAA (Communications Analysis Association) NEWS

By [redacted] P14

What's black and white and red all over -- and has five feet? Or, to ask it another way: Suppose you were asked to explain what your particular corner of the cryptologic garden is really like, to someone who is "in the business" but not in your skill field. How can, say, a cryptanalyst explain to someone who isn't (and probably isn't going to be) just what goes on in the life and work of a cryppie? It seems to me that over the years one of the most difficult communication problems we have had is getting one skill group to really understand what a neighboring one does. If I am never going to *be* a collector (and I'm not), then how can you get your viewpoint through to me, by answering such questions as: "What is it like to be a collector? What things turn you on? What things represent excellence in work to your peers? When you've had a good day, what made it so? How do *you* spot a "pro" in your field when you see one?"

Dave Gaddy came up with an idea about this and what the CAA might do to encourage such communication between disciplines. Imagine, if you will, a Five-Foot Shelf of Great Cryptologic Literature -- but with this proviso: that every book or article on the shelf is aimed at people *outside* the field described. What would you choose?

I've asked several people, and have gotten rather different answers. At the outset, I frankly wasn't thinking about an actual shelf, but more like a bibliography. However, I have been offered (and have accepted) some collections of documents and papers on various subjects.

Do you have any favorites you want to see on the shelf?

Membership Drive: Our Annual October Membership Drive is now under way. If you join now, your dues will be fully paid through the end of next year. That's 15 months for the price of 12, folks!

There's a leak somewhere! The word seems to be getting around. In a place like this, you can't keep anything a secret, can you? CAA members, undaunted by our constantly changing times and places, *have* been finding our meetings. Now that the secret is out, we might as well settle on one meeting place -- the B5 Conference Room (3S040). When? We're not going to make it *that* easy for you. There will usually be a secret clue, in the minutes of each board meeting, about the time and place of the next one. See if you can find it!

P.L. 86-36

At a recent Board meeting, [redacted] President of CAA, submitted a note that contained the following statement that, I think, deserves wider publicity:

"I would like to see us doing things that aid people to grow in their work. Personal growth (that is, becoming better people and better NSA employees, not just getting promoted) is to me a key objective, and, given the cross-disciplinary orientation of CAA, we are in an ideal position to help. Post-professionalization (and even professionalization) is one place where we can get into things like this. Nor do I think we should limit ourselves by a strict interpretation of the limitations of our charter or fear of impinging on management's prerogatives. If we can improve the quality of people at NSA, we have done a service for all."

OCTOBER presentation:

Mike Tilley [redacted]

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

NOVEMBER presentation:

The following are clues concerning the CAA November presentation. Can you match them up? Each number matches up with one of the letters.

1.	[redacted]	A. Found in some homes
2.		B. Found in the Orient
3.		C. Found in some homes
4.		D. Found in the Orient
5.		E. Found in some homes
6.		F. None of the above

For additional clues, watch for the announcement of our November presentation. (CAA members: Check your mailboxes for the announcement.)

P.L. 86-36

For information, call [redacted] President, 1193s, or [redacted] Board Member, 3369s. CAA Board listed in September CRYPTOLOG.

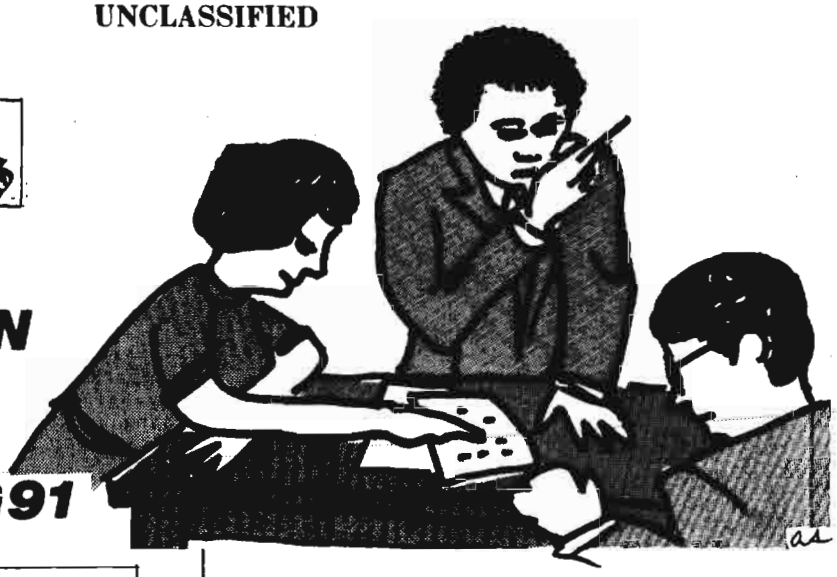
P.L. 86-36

~~CONFIDENTIAL~~

Department of
GOLDEN OLDIES

ANALYZATION OF DATA

G91



P.L. 86-36

The following article appeared in the September 1971 issue of DRAGON SEEDS, an informal B Group publication that has since been discontinued. The article was followed by an editor's note saying "We will have further comment on this article in the December issue of DRAGON SEEDS."

And there was further comment on it -- some of it vehement -- even before the December issue of DRAGON SEEDS appeared. CRYPTOLOG readers who are not familiar with the article might like to figure out what all the ruckus was about. But CRYPTOLOG readers who already know are asked to keep silent, thus letting a whole new group of readers enjoy this classic fully.

Explanatory comments can be obtained by writing to: CRYPTOLOG, P1.

Ed.

An analyst should first study data in its original form looking for obvious or significant points. By all standards it is most important that an analyst look for virtually any and all signs of unusual conditions which could occur in any form, in any data.

Customarily a thorough analysis is a primary goal but prior to any thorough analytic study, much can follow from initial scanning of data looking for virtually any important sign or signs. Do this first! From this point, particularly having run out of initial scanning of data, an analyst who works with traffic should dirty his hands by actually handling and sorting traffic in its original hard copy form.

Going through traffic, occasionally voluminous amounts of traffic, is a duty of all analysts. Having to do this has its applications to follow-on analysis. In this follow-on analysis many sound conclusions may solidify by improving facts first found during initialization. Just to avoid confusion, analysis is not sorting traffic -- it is a logical accounting for all individual parts of a main body of data.

Knowing functions and limits of said individual parts is important. Looking at all parts individually and as a group is always most important. Missing parts could focus on basic primary origins of data. Non-association of parts could add support to analysis also.

Odd or unusual conditions should aid in producing a working copy of an original body from which your data was forthcoming. Primarily, in addition to analysis of data, an analyst must list all significant facts for historical background information. Quick logical drawback of this information is an important point in analyzation. Random approach to drawback of data is not satisfactory in most situations.

Should various arts and skills apply, an analyst must vary his attack accordingly. This is a sign of a good analyst -- pliability or adaptability to situations and changing conditions. Until an analyst displays this quality in his analysis, an analyst is not functioning at a maximum standard.

Vital to all analysis is a thinking analyst, with ability to occupy his mind with various and sundry points. Which point to disavow or disclaim and which to follow up is not always obvious. X-ray vision would aid any analyst, in both scanning of data and looking into goals of tomorrow.

You, as an analyst, occupy a vital position in an analytic community -- much of your analysis is original with no duplication by co-analysts, thus your analysis is primary to analytic community goals and missions. Z-groups and A-groups should aid cryptanalysts in locating indicator or discriminant groups and in turn aid in important cryptologic findings.

(Did you do any analysis of *this* data?)

Letter

[redacted]

(C ~~CCO~~)

Solution to NSA-crostic No. 9

(*CRYPTOLOG*, September 1977), by David H. Williams

P.L. 86-36

[redacted] "[The] Uses of Elegant English" (*CRYPTOLOG*, November 1976):

"It was Engelbert Humperdinck, I think, who sang a song recently, whose lyrics are the epitome of originality and poetic imagery of which today's songwriters can be so proud. 'I'm yours,' sang Mr. Humperdinck, 'till the stars fall from the sky, for you and I.'"

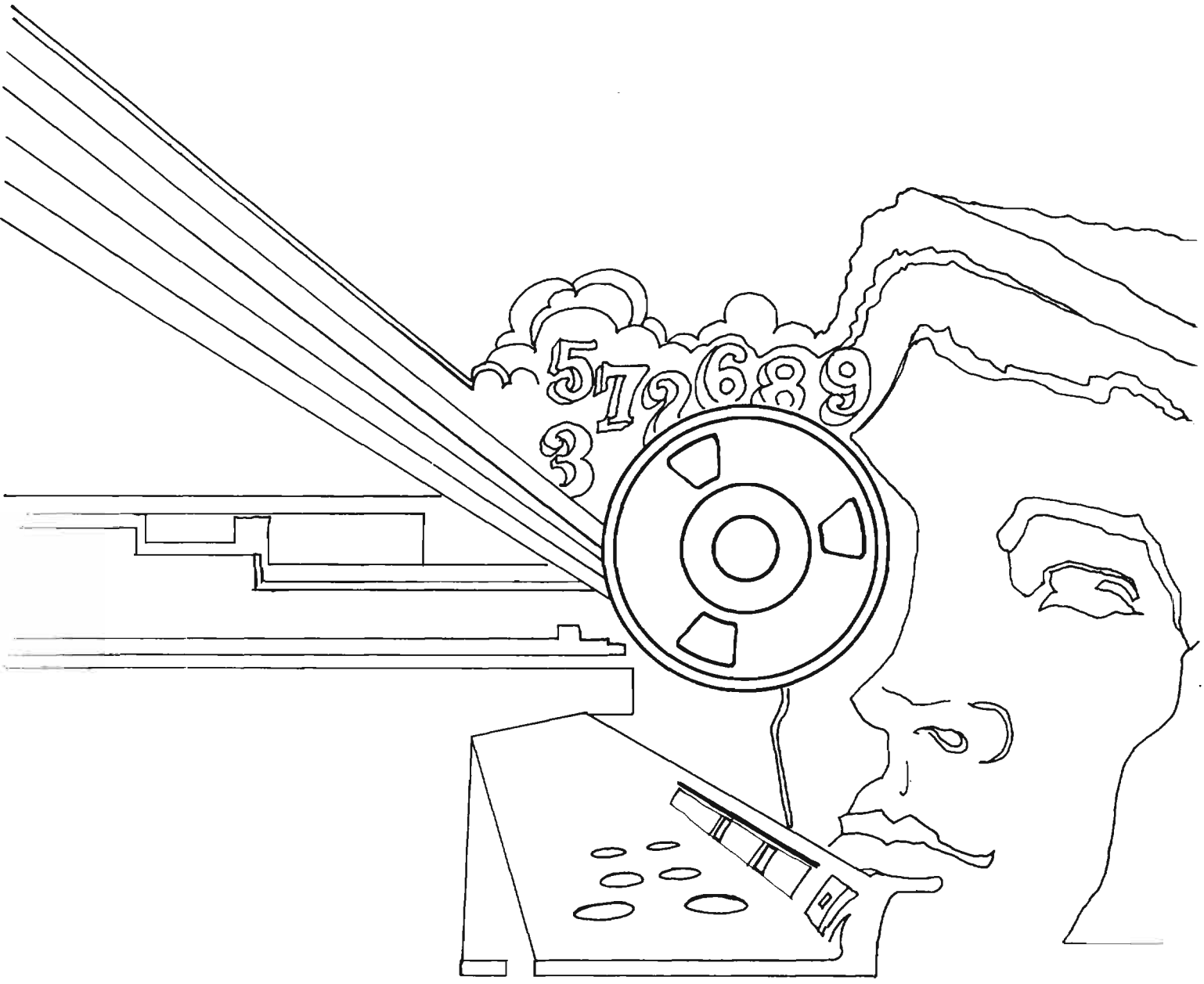
Engelbert HUMPERDINCK
COMPOSER
(Hansel and Gretel)

(U)

[redacted]

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

P1-SEPT 77-S3-25519


5 7 7 6 8 9
3