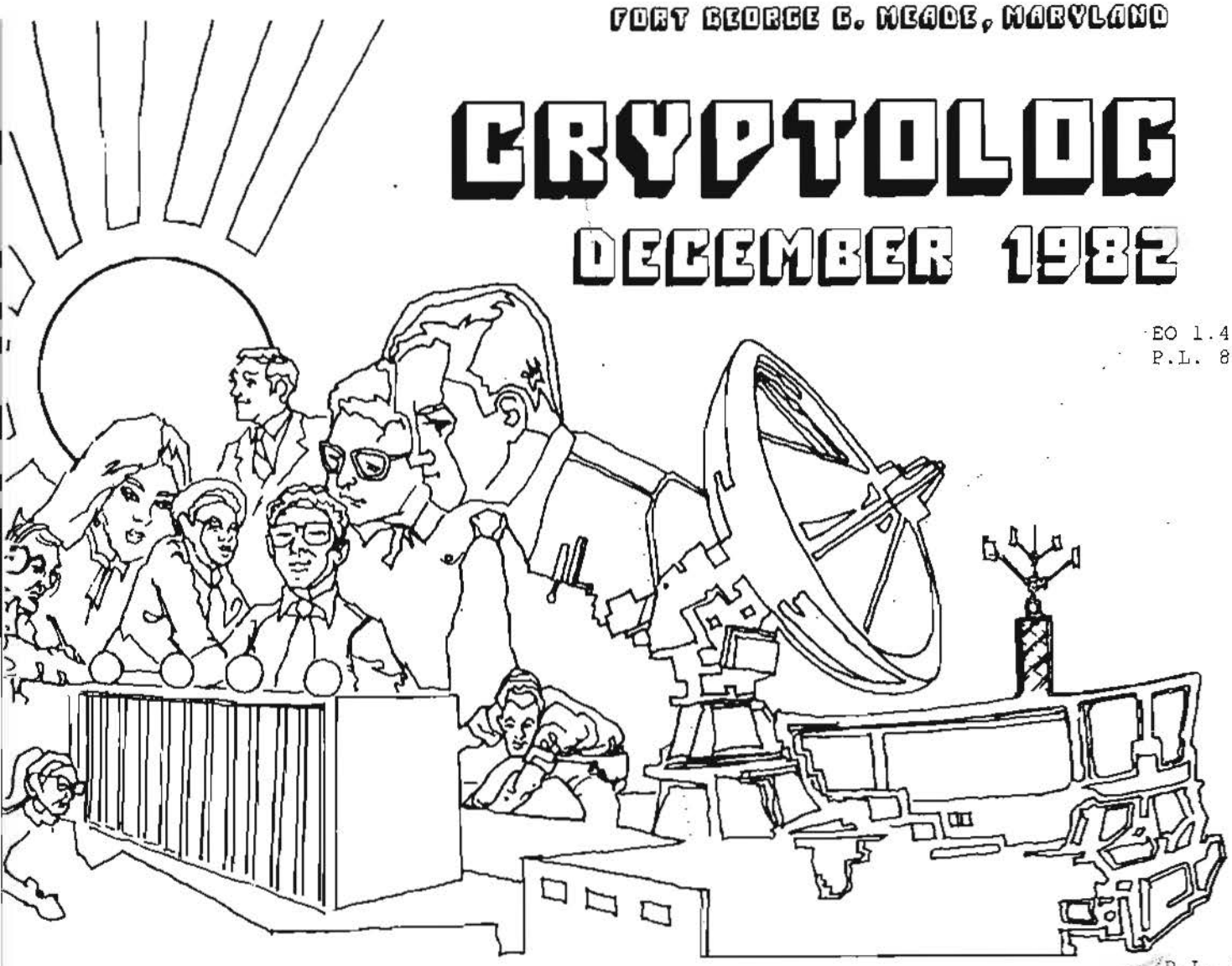
~~TOP SECRET~~

I423 [redacted]

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

DECEMBER 1982



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~
US/UK/CAN/AUS/NZ EYES ONLY

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. IX, No. 12 DECEMBER 1982

For subscriptions
send name and organization

to: CRYPTOLOG, P1
or call [redacted]3369s

P.L. 86-36

To submit articles or letters
via PLATFORM mail, send to

cryptolg at barlcØ5
(bar-one-c-zero-five)
(note: no '0' in 'log')

Editorial

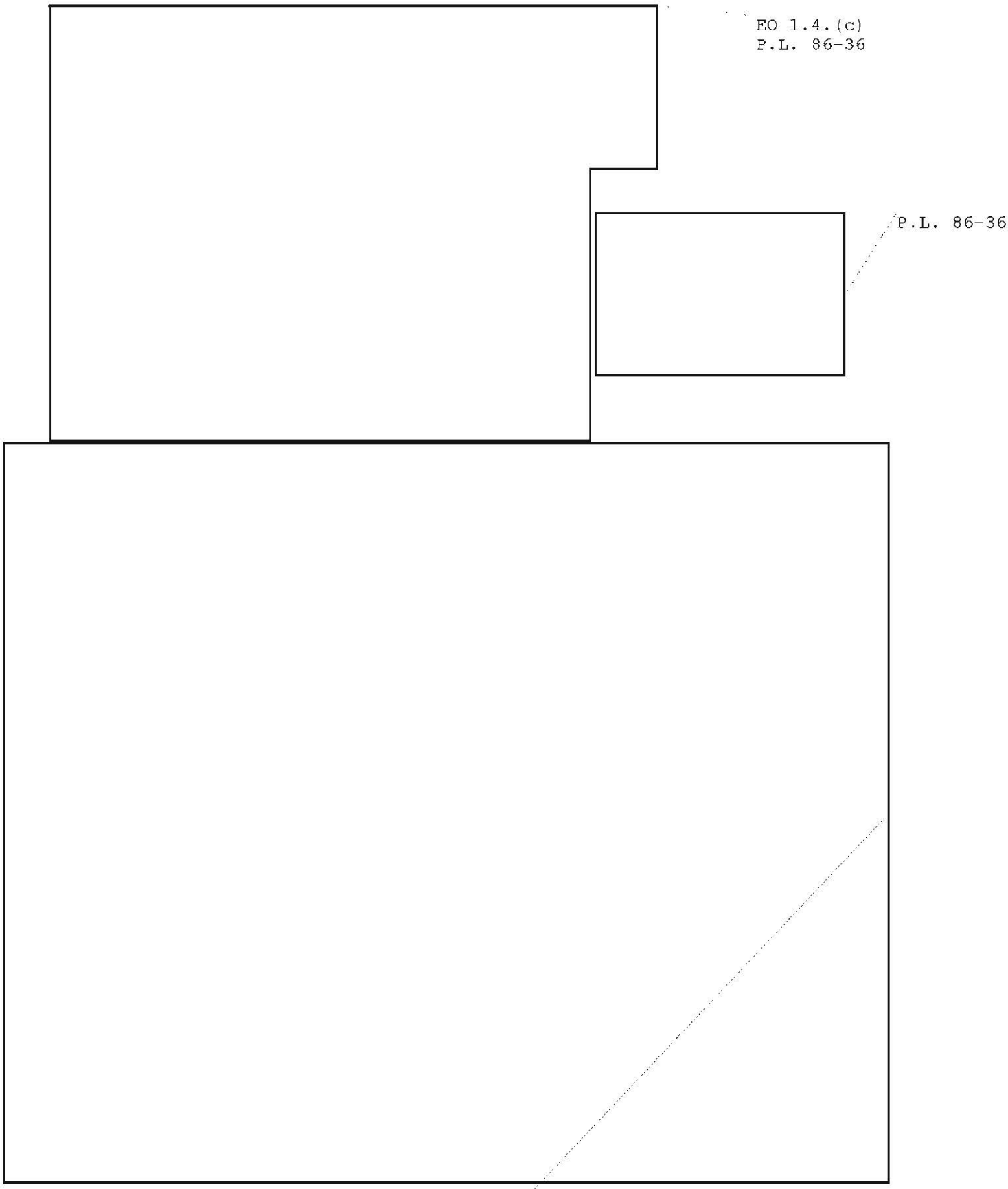
It is undoubtedly a coincidence, but just three weeks after our editorial appeared about moving, we were notified that WE were moving. There is something about moving that is, frankly, unsettling.

It must be said that the people one encounters when moving are quite friendly and helpful. The telephone people, for instance, must spend much of their time having to deal with people who are unhappy about having to move, yet they were sunny in disposition (more so than I would be if my job required me to deal continually with displaced persons). And so, in fact, were all of the other folks we met along the trek.

Moving can be an adventure. I have fond memories of long columns of desks, moving slowly at the command of column coordinators with walkie-talkies. And there are advantages to moving: it is a good time to throw away some of that accretion of stuff that I keep accumulating.

Besides, if [redacted] is right (CRYPTOLOG, June-July 1982, p25), then somebody has to move! So as long as whoever keeps the roster does it fairly, my turn will only come up every so often. Of course, if I could figure out how that roster works, maybe by getting myself transfered at just the right time, I could stay in one place and let the new organization move in around me!

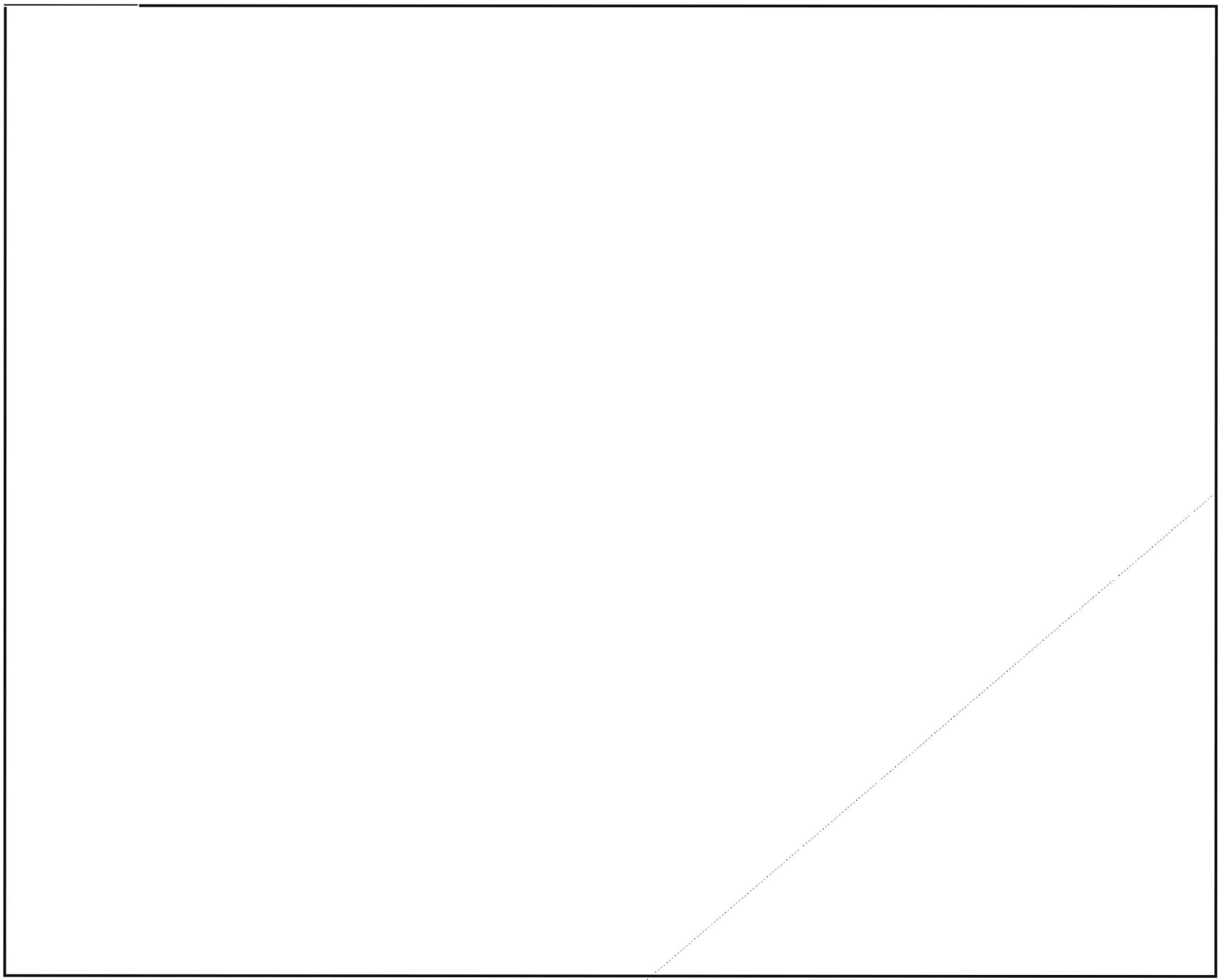
Next month, something different...



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

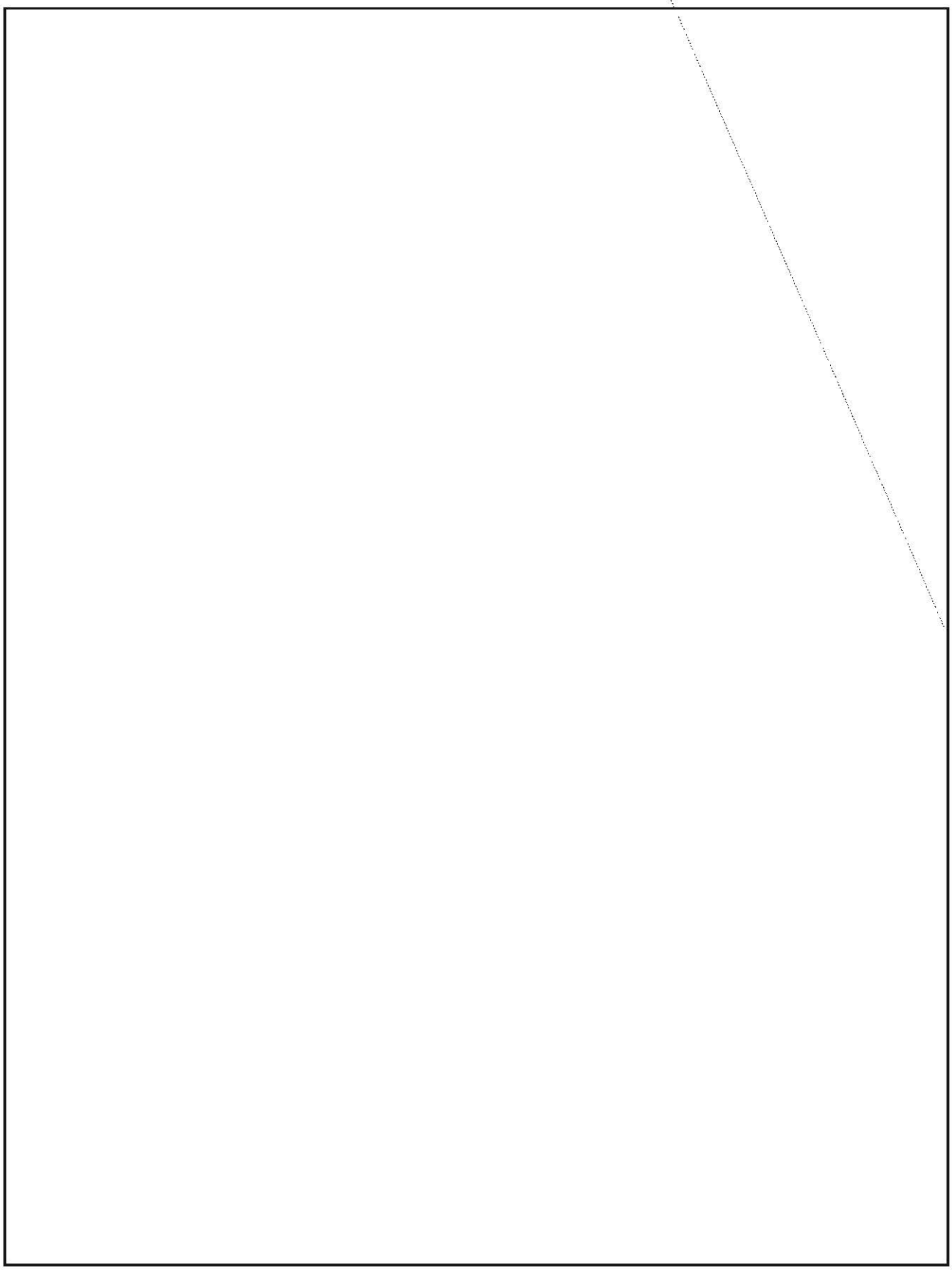
P.L. 86-36

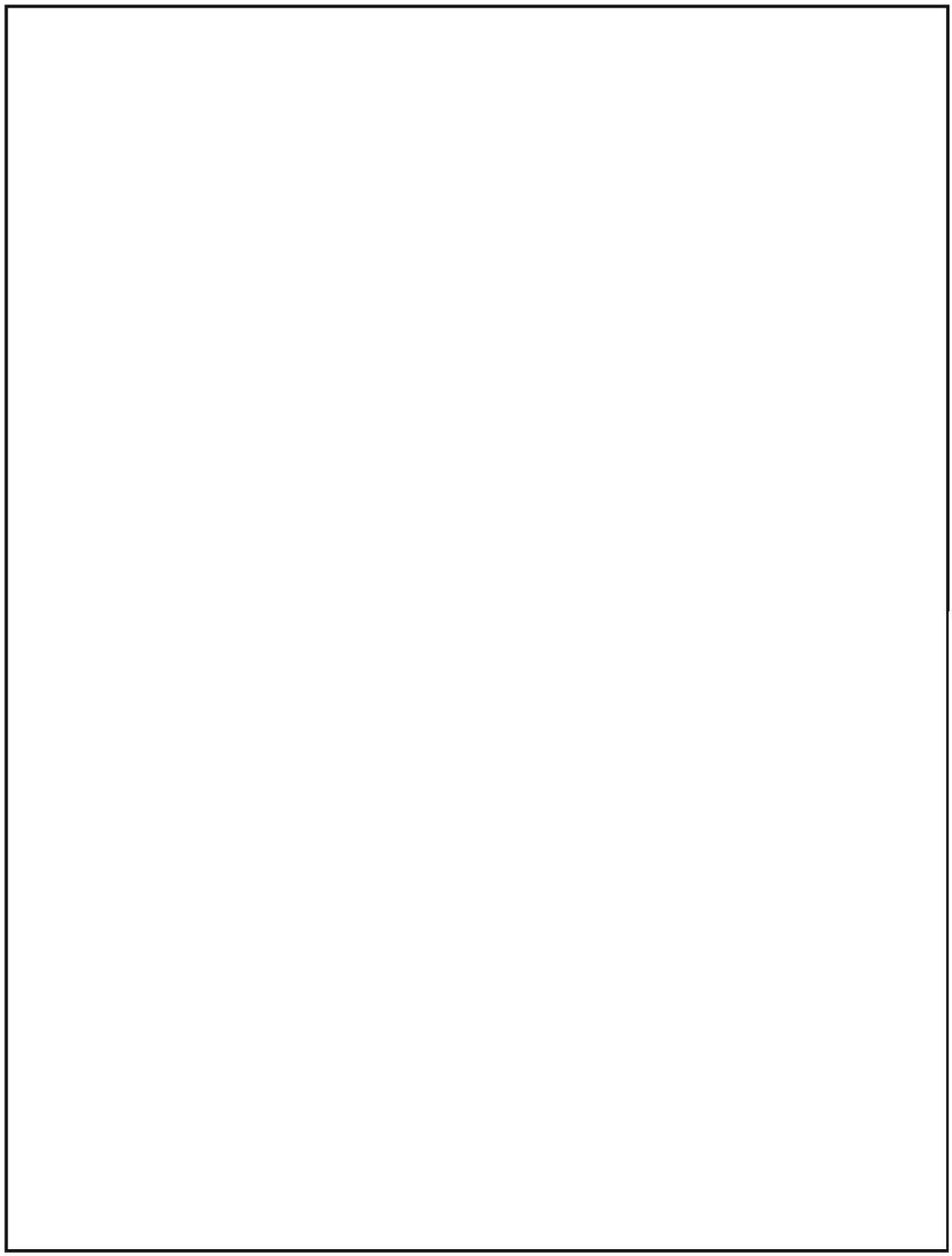
EO 1.4.(c)
P.L. 86-36



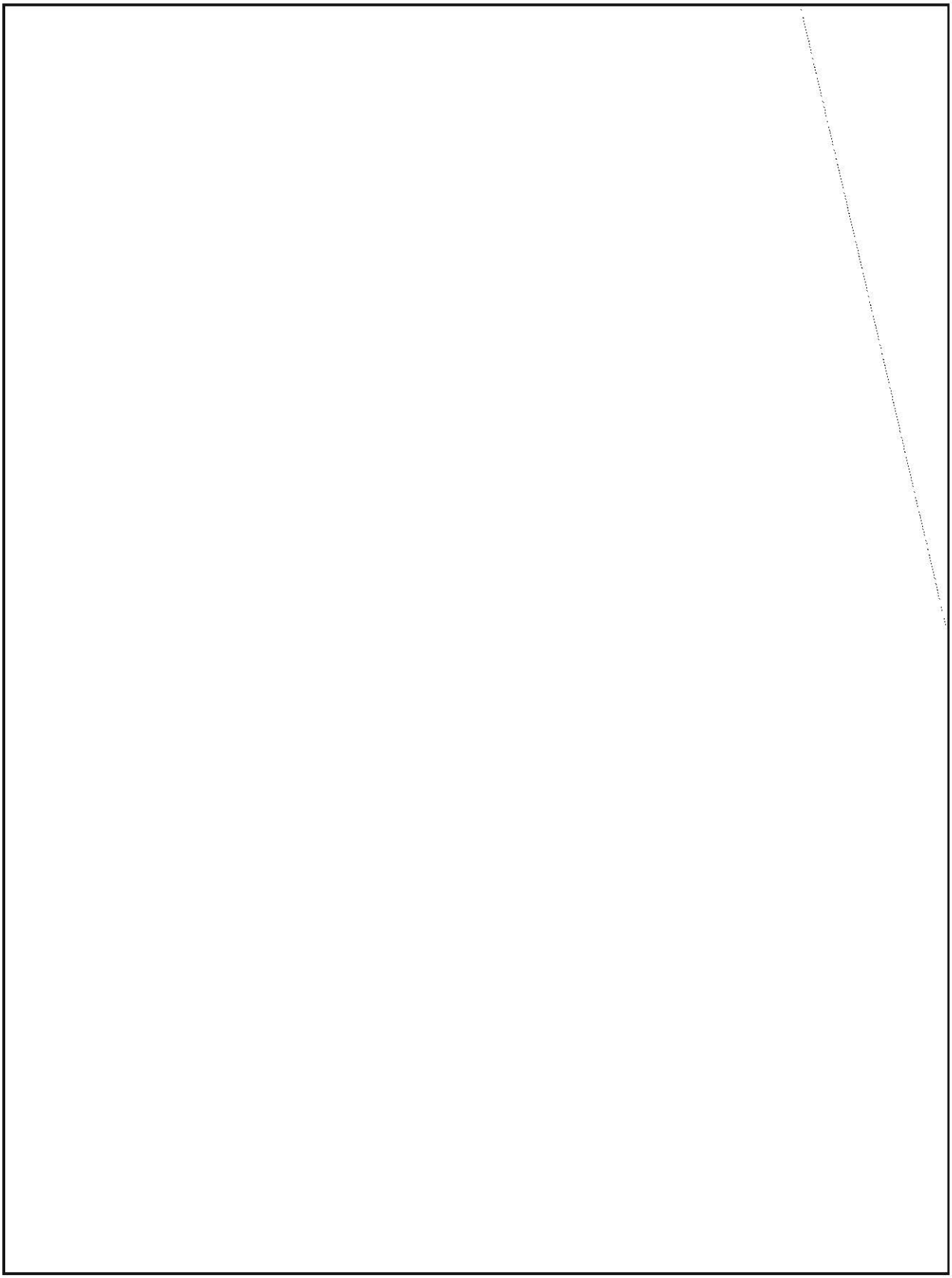
EO 1.4.(c)
P.L. 86-36

~~TOP SECRET UMBRA~~

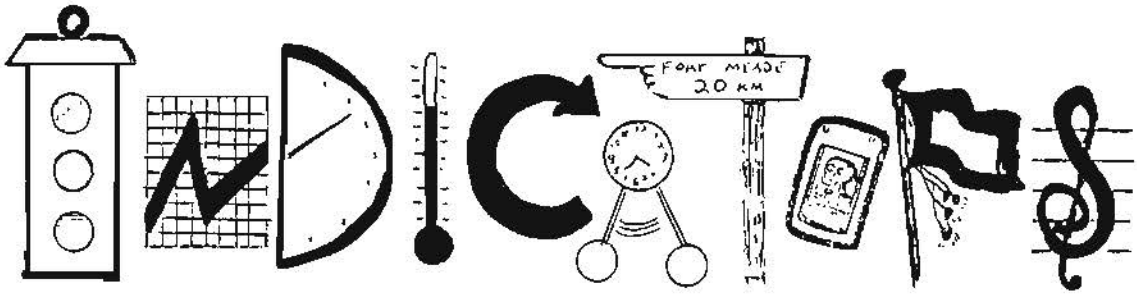




EO 1.4.(c)
P.L. 86-36



The Development and Correlation of



by [redacted] S24

P.L. 86-36

Warning indicators postulate specific actions that a foreign power may take prior to the initiation of hostilities. Indicators are ~~(C)~~ developed from collected intelligence, historical data, and the political and military doctrine of a foreign power.

~~(S)~~ Indicator lists are formed by correlating indicators under specific categories; they are used by indications and warning (I&W) analysts as a tool to determine if a possible strategic warning environment is developing. These lists denote the capabilities of specific targets. Those capabilities include known and suspected economic, technical, physical, and military abilities. [redacted]

[redacted]

~~(C)~~ With the indicator list being a tool for warning, the scale for warning is the norm, the target's normal level of activity. I&W analysts use indicator lists to determine if current activities in their area of concern deviate significant from the normal level of activities. [redacted]

~~(S-CCO)~~ To develop indicators from historical data, I&W analysts study the involvement of specific targets in military action.

Indicators based on normal activity are developed from the actions that lead up to the preparations for deployment of forces for an invasion or exercises, as well as from the actions observed during those events.

~~(S-CCO)~~ Developing indicators from a target's political or military doctrine tells I&W analysts what the target may do to prepare for hostilities.

~~(S-CCO)~~ Sources for indicators include all the major intelligence collectors and sensors employed by the US.

~~(C)~~ The development and correlation of indicators is very important to warning. Indicator lists are developed from collected intelligence and the analysis of a foreign power's actions and doctrine. The sources of indicators are the intelligence collectors and sensors that the US employs in its defense. Indicator lists air I&W analysts in determining the status of a foreign power's military capability that decision-makers need to know in order to make the necessary decisions to protect US interests.

A Cry for HELP or Does Anyone Here Remember PURPLE?

by [redacted] P.L. 86-36

(U) During the course "Japanese Cipher Devices Through World War II," which was a part of SPICE (the Summer Program in Intensive Cryptologic Education), some questions arose which neither the teacher nor students could answer. Two of those questions will be posed in this article, with the promise of future articles with additional questions and explanations of the systems involved.

~~(C)~~ There were two goals in the course. The first was to study the history and solution of Japanese cipher systems before and during World War II. The second was to try to solve the Japanese systems with our modern techniques.

~~(S)~~ The students accepted the challenge to treat a set of World War II messages as unknown cipher. The results of the statistical tests were not what the teacher (the author of this piece) had expected to see, based on her research of how the systems worked. The problem was that the messages which she had pulled from the Cryptologic Collection and typed onto the system did not all possess the properties that had originally made solution of the systems possible. It was necessary to tell the students what was supposed to have happened and then try to figure out why the runs had come out as they did.

(U) The class watched the tapes of Frank Rowlett's talk on the solution of RED and

PURPLE, and of Frank Raven's recent talk in the Friedman Auditorium. These analysts imparted the excitement in achieving the original solution, but students and teacher felt that both men underemphasized the difficulty of this achievement.

~~(C)~~ The material in the Cryptologic Collection on RED was understandable and the students were able to solve the messages, given how the systems worked. It was not clear how the original analysts constructed the device from the cipher solution but one student wrote a program simulating RED motion.

~~(S)~~ The material on PURPLE was difficult and the explanations of the system's solution left certain questions unanswered. The first concerned the initial analysis of the system. The World War II analysts had the plain text for parts of 15 messages. In an intensive cryptanalytic study of these messages they found that the number of repetitions was much smaller than would be expected at random. Repetitions of three or four letters never represented the same plaintext letters. Conversely, two identical plaintext letters in sequence could never be represented by two identical ciphertext letter. Friedman writes, "This phenomenon turns out to be the undoing of the machine." [1] However, he does not explain how the lack of repetitions was exploited.

~~(S)~~ The second question concerns the solution of the system. The original analysts felt that they needed 20 to 25 messages with the same indicator on the same day to solve the system. They never found more than two messages that satisfied these conditions. Another idea was to convert messages with the same indicator, but on different days, to a common base. Out of a thousand messages, six were located with the indicator 59173. When reduced to a common base, these six messages became the key to the breaking of PURPLE. Friedman describes the process as "too difficult to explain here." [2]

~~(S)~~ The two unanswered questions are:

1. How did the analysts use the repression of repetitions in solving PURPLE? and

2. How were the messages with the same indicators, but on different days, reduced to a common base?

~~(S)~~ Further questions can be posed in an article which describes the system. In addition, there is a course in the Cryptologic Collection on PURPLE with explanations and assignments. Though most of the explanations were understandable and the answers to the problems in the assignments were provided, something was lacking because the problems did not seem solvable.

~~(C)~~ Is there anyone at the Agency who worked with PURPLE or who once studied the PURPLE course material? Would anyone like to help resolve these puzzles? Could modern techniques solve the systems today? Please contact [redacted] B63, on extension 4871s. P.L. 86-36

1. Friedman, William, "Preliminary History of the Solution of the B Machine," p. 4.

2. Ibid., p. 5.

WE ARE ALWAYS LOOKING FOR

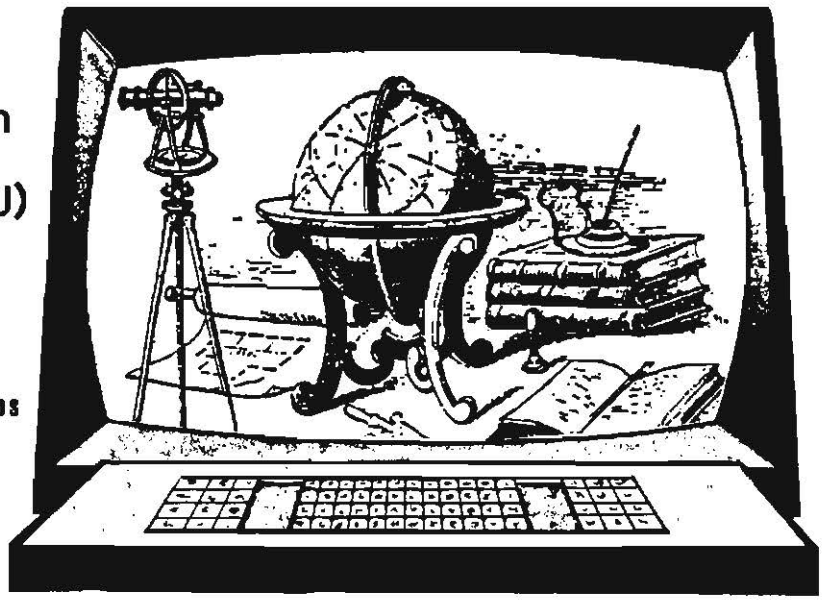
ARTICLES, COMMENTS, NOTES, LETTERS,

THAT WOULD BE OF INTEREST TO OUR READERS

Going *On-Line* With Information Aids (U)

by Jack Gurin, (R831)

Systems Research Labs



That we are in the information age is no longer debatable. For some years now we have been aware of the impressive advances being made in the business of acquiring, storing, retrieving, and displaying information. We are also assured that there is much more to come--smaller, better, faster--and we have no reason to question that claim. It is exciting to contemplate the possibilities, and not a little scary. Even if we wished to slow down or stop the process, there would be no way to do it, and so we speed along with the current.

Of course it is the computer that is in the middle of the information explosion, and it is the computer that enables us to sit at home or in an office and be the recipient of all sorts of facts and figures, provided that we have subscribed to the appropriate service. If we really wanted to, we could see the entire daily New York Times on our screen by 0800 each morning, but there are better ways to read the paper. On-line information services crisscross the country and there seems to be no limit in the kinds of information that may be provided. Too busy to read all the magazines and journals affecting your area of interest? You can subscribe to a service that summarizes all the information for you. Reluctant to plow through all the stock market information in the papers to see how your investments are doing? You can be served precisely the information you need on a regular basis. The on-line services cater primarily to businesses, as one would expect, but the range of information available in all fields is impressive and it is growing all the time.

It is in the cards that the computer will be asked to provide more and more answers to questions asked in the course of SIGINT analysis, and yet there remain many questions regarding the advantages of on-line versus off-line information support. It isn't easy to visualize a familiar operation like looking up a word, a person's name, a place name or an abbreviation without the comforting reassurance of dictionaries, working aids, gazetteers, and other friendly reference works. It will take heavy-duty convincing to get some people to agree to give away their books and rely instead on the flickering images of that close relative of the medium that brings us "Charlie's Angels."

We need to discover just how valuable on-line information would be for SIGINT analytic processes. Speculation will take us only so far, and we need to know for sure how useful it would be to have answers to our questions provided on the screen. Would it take less time? Would the answers be more accurate and complete than if one proceeded in the traditional way? What would this do for SIGINT productivity? Output quality? How would the individual transcriber or analyst react? How valuable would it be for the linguist to be able to look up a the meaning of a word when he does not know either the beginning or the ending? What about place-names and maps being displayed on the screen? Or charts and diagrams? In our planning for large-scale systems of the future, what should our requirements be for on-line information support? What will it do for (or to) the individual sitting in the middle of the system?

The answers to these and related questions are being sought by KEPLER, the laboratory in R83 that is working on a design for the ideal transcriber work station. In April and May of 1982 a test was conducted in operational spaces, employing two transcriber teams in A67 who continued to work on their regular traffic. A group of six information aids, some of them the most frequently used by transcribers, were made available in computer-retrievable form to the transcription teams. Experimental equipment was brought in to display answers to their queries on-line, and while one team used the experimental positions, the other operated in normal fashion. Periodically the teams reversed roles and all the while trained observers were watching the operation and collecting data to permit an evaluation of on-line aids in the transcription process.

It became apparent almost from the outset that the experimental on-line information aid system, nicknamed WALDO, would quickly become a favorite reference device for most of the transcribers participating in the test. WALDO, to the transcriber, was a second DD7000T screen that was controlled by the same keyboard that was used for creating transcripts. It was connected to a minicomputer that contained the information aids. The transcriber could and did ignore all of the experimental equipment but the second screen. The retrieval system was designed to be attractive and easy to use, and that WALDO was a most welcome tool is evident from comments made by the transcribers in their End-of-Test Questionnaires:

√ "Easier and faster than paging through hardcopy."

√ "String-search allows scribe to look up words even when portions are unknown--a big help."

√ "Fun to use."

√ "Caused scribe to look up more entries, thereby improving quality of work."

√ "Dread going back to STEPSTONE alone."

√ "Makes STEPSTONE look primitive in comparison."

√ "It would be great if we could incorporate WALDO/KEPLER into our permanent operations for the whole branch."

√ "I hope this helps get us all on-line working aids because I feel the time we save using these aids is time we can use to concentrate on our ever-increasing workload. I know I've said this before, but I just can't get over how convenient and easy this on-line system is. If all the working aids that we use with any frequency are put in WALDO, then we'd have that much more space in our desk."

√ "With the ORTHO on-line, I find myself using it at least 10 times more than if I had to drag out that book for every jumble of sounds I heard. It is easier with WALDO to try the various configurations of letters to see if a legit word turns up. Paging through the orthographic hardcopy was something I unfortunately avoided, which left blanks in my transcripts. But I find myself now filling in more blanks because it's easier to do with the orthographic on-line. I think my work has definitely improved!"

The observers who noted how aids were used during the test found in general that, when an information aid was available on-line in the experimental mode, it was used more frequently than its hardcopy equivalents in the control mode. Also significant was the finding that the average durations of aid use by transcribers tended to be shorter for on-line than for off-line aids. It should be noted that these savings were in worktime per individual query and did not necessarily result in a savings in tape processing time. It is likely that, because it is so much easier and quicker to find answers in on-line aids, many more queries will be made than when only off-line aids are available. This would probably offset some of the savings in time but might do wonders for the quality of the product.

In addition to determining that on-line aids were used more frequently and took less time per query, it was also found that the subject transcribers were unanimous in preferring the on-line version of most WALDO aids to any alternative form.

While the results were far from conclusive in the calculations of the transcription work

factor, there were strong indications that working with on-line aids had reduced transcription time as much as 18 or 19%. In view of the limitations of subject population, targets, and time, however, it is difficult to predict the probable impact of on-line aids on the transcription work factor in other target areas.

In a related but separate subtest, 150 terms were selected randomly to determine how quickly one could look them up using WALDO versus using equivalent hardcopy or microfiche aids. Simulating operational conditions, both experimental and control, the tester kept track of the times it took to look up each of the terms on WALDO and on six off-line aids. He found that on-line retrieval times were generally faster than other times. This finding came as no surprise for those aids that are located away from the work area, in which case the on-line answer could be provided in as little as one seventh of the time. The unique characteristic of on-line files, that of providing the opportunity to look for terms without knowing how they begin and end, was not tested because there was nothing in hardcopy or microfiche with which to compare it.

What happens next? There is little doubt now that on-line information aids are a GOOD THING and should become a standard feature of all workstations. It also seems that the effort and cost involved in preparing aids for on-line retrieval would be, in many cases, quite modest since a surprisingly large proportion of all hardcopy aids are produced through computer word-processing and therefore exist in digitized form. But it will take a commitment on the part of systems planners and managers not only to bring in on-line aids but to follow through, for many of the aids require updating and new ones are waiting to be created. Perhaps what is needed is more evidence that on-line aids pay off handsomely in raising both the quantity and quality of the end product, and proof that transcribers, translators, and analysts would find their work so much more rewarding with on-line information aids that they would be reluctant to leave for other types of employment.

The KEPLER experiment and test was directed toward the needs of transcribers, but the principles and techniques are capable of much broader application. It is characteristic of almost any analytic activity that the practitioner consult reference materials. It also seems reasonable to assume that it would be highly desirable to make the retrieval of the information easier, faster, more timely, and more complete, all likely results from an effective on-line information system.

How did they ever make reservations on the airlines before computers?

SOLUTION TO NSA-CROSTIC No. 44

[redacted] "Language [in the News], CRYPTOLOG, September 1974. P.L. 86-36

"When Archbishop Casaroli, Vatican Secretary of State, came to Warsaw to consult with the Polish Foreign Minister, [he] spoke some Polish...'Let God guard Poland and lead it to great and happy goals,' he said, adding, 'Niech zyje Polska!' ('Long live Poland!')"

From: djh at ERMELIN
Subject: Cryptolog subscription
To: cryptolg at barlc05
cc: djh

I'm tired of borrowing copies of Cryptolog and would appreciate receiving my own copy. Thanks.

[redacted] P.L. 86-36
R722

QUESTIONS IN SEARCH OF A PQE (U)

by Jasper T. Schmedlapp

Here are the five questions submitted by the author for the Computer System Analyst certification exam that never saw the light of day at the end of the tunnel. Choose the best answer, break your #2 pencil when done, and then look up.

1. What are the chances of project success, in a matrix management environment?

   a. Slim and none.

   b. It's fine for small projects.

   c. It's fine for large projects.

   d. Actually, it's the individuals assigned that make the difference.

   e. Good, if you stick like glue to 81-2 and 81-3 is your apogee.

2. According to a current book about the agency, how many computers are there in the basement?

   a. Not too many, since the roadway is 100 yards wide.

   b. Enough to decrypt the boss's handwriting.

   c. It's classified, but the main ones are CARRILLON, STARFIRE, LOADSTONE, and WINDHILL.

   d. Just as many as they can possibly fit in, and then some.

   e. One for every man, woman, and child in (pick a county in the state of Maryland).

3. Just what is Computer Programming anyway? It's...

   a. All just 1's and 0's.

   b. An arcane art that Macbeth's witches would have enjoyed.

   c. A way to make a living.

   d. Where a man belongs.

   e. A hell of a lot of fun when we do it, instead of everything else involved.

4. If the program doesn't work, what to do?

   a. Run it again, just to be sure.

   b. Ask the gang in the carpool.

   c. Hope that that case never comes up.

   d. Consider using "GO TOs".

   e. Come back to it tomorrow with a fresh mind.

5. In 1's complement arithmetic, +0 = -1; are the operations "minus" and "nonplused" also equivalent?

   a. Only on the CDC peripheral processor, which has 4000 words of memory.

   b. Yes; but in Burroughs ALGOL, it's much more elegant.

   c. The C language doesn't make this distinction and many others.

   d. Why not try it and see? After all, life is an open-book exam.

   e. No, but be careful for it in your local TELNET command language.

To find the answers, look deep within your heart and pick the first things that float to the top of your head.

SHELL GAME:

COUNTER by W.E.S.

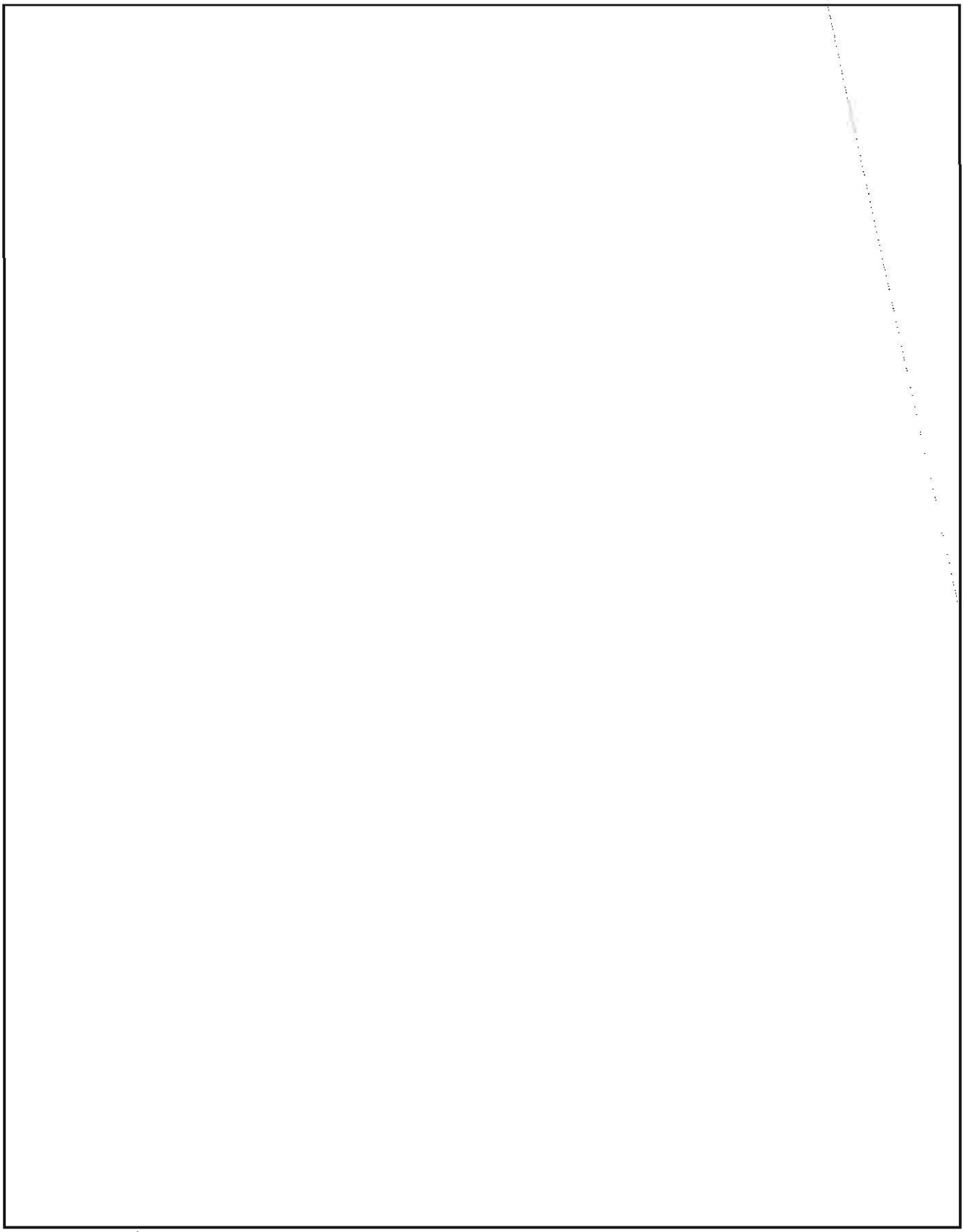
AJSQUE by [ ] P14

P.L. 86-36

PWB WHEN by [ ]

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

(S-CCO) UNIX is not known as a good command language for arithmetic operations. Most sophisticated calculations probably ought to be done by some other means. That doesn't mean, however, that nothing arithmetic can be done in UNIX.



P.L. 86-36

~~(C-CCO)~~ Reminder:

if you have any old codes or code materials, such as runs or tapes or cards or write-ups, and you're looking for a good home for them, I'll be happy to take them in. [redacted] also accepts such material. His address is T54, SAB 2 Door 3, and he can be reached on x2268s.

[redacted]
P16, x1103s
Bookbreaking and Cryptolinguistics Coordinator

To: Editor, CRYPTOLOG

Dear Ed:

Kudos to [redacted] for his perceptive, albeit scary, series on "SIGINT: 1990." He graphically lays out the challenges facing the SIGINT folks of that era, which is rapidly becoming more and more imminent. The table in the November article displaying the 64 teleservices envisaged by the French CNET study for the year 2000 can set one's mind adrift on a sea of imaginings in the sphere of social relationships, too. For example, a young bachelor of that day might embark on TELESURVEILLANCE to check out the field; or if that fails, there are TELEWANT ADS or TELESHOPPING as prelims to his TELECOUPLE adventure, followed perhaps by TELEGAMES together--and then, sadly, by TELESWAP (if ardor cools)... The TELEpossibilities boggle the mind.

[redacted] P13

P.L. 86-36

KRYPTOS Society: Distinguished Members and New Seal(U)

P.L. 86-36

by [redacted] S14

At the 14 September 1982 meeting of the KRYPTOS Society, President [redacted] announced the names of the first 14 Distinguished Members of the Society. The initial group was selected from a list of over 100 candidates. Selection criteria were based solely on cryptanalytic skills and achievements. To be eligible for consideration, a candidate must have retired since 1935 from the "official cryptanalytic community" in the United States, Great Britain, Australia, Canada, and New Zealand. The following were selected:

~~(S-CCO)~~

[redacted]
William Blankinship
[redacted]
Prescott Currier
[redacted]
William F. Friedman
Hugh Gingerich
Solomon Kullback
Francis ("Ted") Leahy
[redacted]
William Lutwiniak
Francis Raven
Abraham Sinkov
John Tiltman
[redacted]

P.L. 86-36

(U) In the future the KRYPTOS Society will publish a paper describing the achievements of these Distinguished Members.

(U) At the same meeting [redacted] Chairman of the Logo and Seal Committee, presented the seal of the Society, which is based on the Gordian Knot. The following is Joe's version of the story:

(U) Once upon a time in the ancient kingdom of Phrygia, the government had many problems, the most immediate of which was to choose a new king. So the high officials went to consult the leading local oracle for advice on whom they should select for their king. The oracle gave them the following astonishing advice: "Choose the very next person who approaches the Temple of Zeus in a wagon. Then all will go well for Phrygia." (History does not record how much the oracle was paid for this advice.)

(U) Along come a country farmer named Gordius and his wife, driving their oxcart into town and they pull up in front of the Temple. You can imagine Gordius' surprise when he is surrounded by government officials and other well-wishers heralding him as king. Well, Gordius was quite thrilled, to say the least, and to show his gratitude he tied his oxen to the Temple with a beautiful and intricate knot. In fact, the knot was so intricate that no one could untie it. Years went by, and still no one was able to untie it. Centuries went by, and still no one could untie it, so that the legend grew that that the knot could be unraveled only by the one who was to be the conqueror of Asia. According to the story, when Alexander the Great invaded Phrygia he was shown the Gordian Knot. He took out his sword and--in true, pragmatic, cryptanalytic fashion--slashed it apart.

(U) [redacted] was the one who suggested the Gordian Knot as the theme for the Kryptos Society seal. He also suggested that it could be portrayed in the form of a shield with three important elements depicted on it: the knot, a sword, and a helmet. The knot depicts the cryptanalytic problem; the sword depicts the tools of the cryptanalyst; and the helmet symbolizes the cryptanalyst--the helmet being a symbol of anonymity. The seal that we see today incorporates those three elements and adds the word KRYPTOS (Greek for "hidden" or "secret") across the top in Greek letters. The shield was designed in its present form by [redacted] of L23 and professionally rendered by [redacted] of L2.

P.L. 86-36

m#4Jb:A7wkSEs ???

XsH8|5gP2:K% ???

6I|mUDu&s-40 ???

PASSWORDS(U)

by [redacted] P13

P.L. 86-36

The author's address for PLATFORM mail is mary at mycroft.

While reading [redacted] excellent article in the October issue of CRYPTOLOG (p. 6), I could not help becoming more and more unhappy under my "human factors hat." The article describes a recent compromise of a password file in one of our computer systems. It shows that the passwords, even though encrypted in the file, could easily be recovered by guesswork. It advises users to cooperate with the intent of protecting passwords by choosing passwords that "will not fall out through a simple analysis effort." In order to make passwords harder to guess, [redacted] offers advice I will paraphrase as follows:

- the longer the passwords are, the better;
- increase the alphabet size, for example, by mixing upper and lower case characters, numbers, and punctuation.

This is all good advice, when we are maximizing only one value: that of making passwords as secure as possible. Unfortunately, the average computer user has multiple goals in his use of a computer system, only one of which is prevention of unauthorized access. All of us at NSA are all too aware of the crucial importance of security. Passwords are still a pain in the neck to most of us, constituting one more obstacle between us and our work at the terminal. We know they are necessary, but we also know that our lives are a lot easier if our password is

- short,
- easy to type, and
- easy to remember.

P.L. 86-36

Alas, we see that [redacted] good advice flies directly in the face of normal human factors design guidelines: to make passwords hard for potential trespassers to guess, we must make them even harder for ourselves to remember and type correctly! [redacted] notes rather plaintively that "there is not a single upper case character" in the 107 passwords recovered from the compromised list by guessing. There are good reasons for that absence of upper case characters, from the user's point of view:

first, it's hard to recall which letter or letters were upper, and which were lower case, especially in the meaningless nonsense-words (e.g., "vkjrd") that are recommended as the best passwords;

second, the shift key is a great error-maker in all typing, since it forces you to use two keys where one would do. All this guarantees that, if you create a password like "vKJ.r-dX", you will probably have to type it over several times before you get it right.

Computer Security folks may be saying "tough!" with little sympathy, since they are interested only in security. I can't quite look at it that way. I think we have to remember that productivity, efficient accomplishment of our jobs, and good morale are also important values we need to maximize.

I don't know what we can do about this conflict of interest between computer security requirements and user friendliness. I can't help wondering why user identifications (initials, organization) couldn't be enough to establish the necessary access restrictions and permissions when tied to user profiles or tables stored in the system software. Why do we need to depend on passwords at all? Might there not be other ways to enforce security at less cost to users?

I suspect that this is only one of many similar conflicts in our software, some far more expensive to users than unlearnable, untypable passwords. My intention here is just to point out the conflict. I am sure some of you could report similar situations, where file security, access restrictions, etc., create real problems for users in the way they are implemented. Those readers in the Computer Security business will doubtless have plenty to say on the other side of the issue. At any rate, I invite readers to send in their ideas on the topic of User Friendliness and (or versus, if you prefer) Computer Security to me [redacted] for inclusion in a future issue of the SIG/Human Factors Technical Notes and/or CRYPTOLOG. (Ed Note: what about using two passwords and letting the system combine them in some periodically changing way?)

P.L. 86-36

HUMAN FACTORS TECHNICAL NOTES

The Computer and Information Sciences Institute's Special Interest Group on Human Factors, chaired by [redacted] publishes a series of technical notes covering a wide range of topics of interest to anyone who wants to keep up with the growing field of human factors. The editor of the notes is [redacted] whose name and articles you have been seeing on these pages.

P.L. 86-36

Some of the articles in the Human Factors Technical Notes have been republished here in CRYPTOLOG, but if you want to keep up with the latest news, you should call Mary on x8845s (or send her a note via PLATFORM using the address 'mary at mycroft') and have your name placed on her mailing list.

The most recent issue contains reviews and comments about recent articles and papers, including:

- Ergonomics of Visual Display Terminals
- Human Factors Standards for Terminals
- Workplace Design
- Windowing vs. Scrolling on a Display Terminal
- Experiments with Terminals and Eyestrain
- Why Alphabetic Keyboards are not easy to use
- Furniture and Posture Problems
- Modelling Computer Data Entry
- Structured Menus

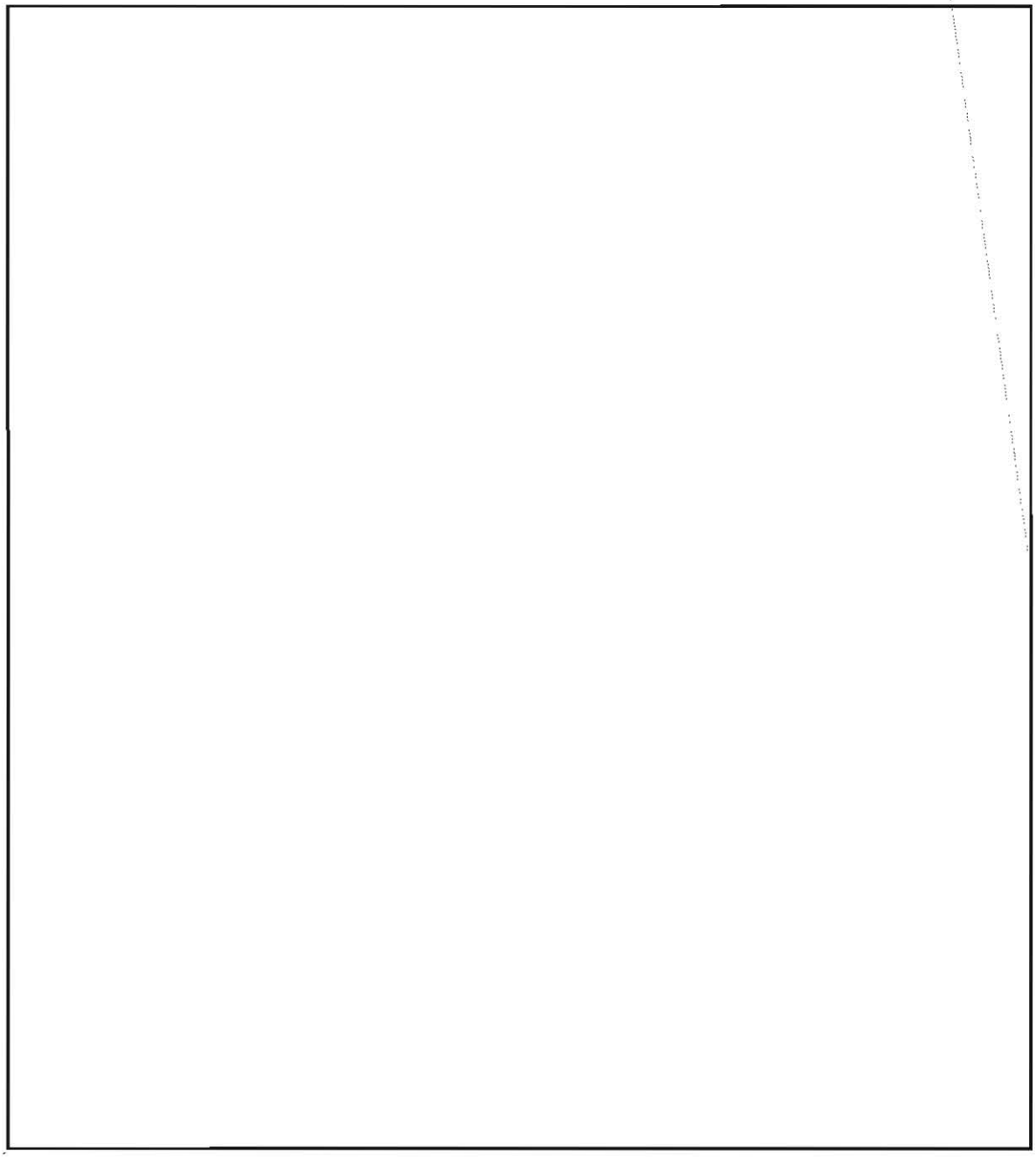
~~CONFIDENTIAL~~

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

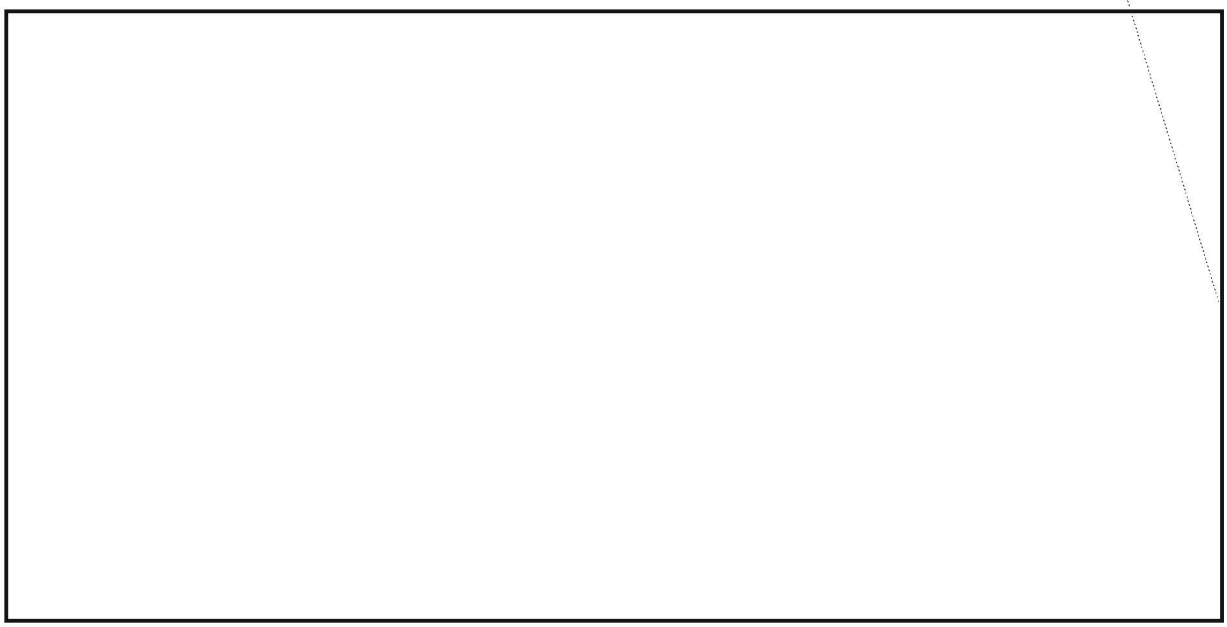
NSA·CROSTIC No. 45

BY REED DAWSON (Retired)

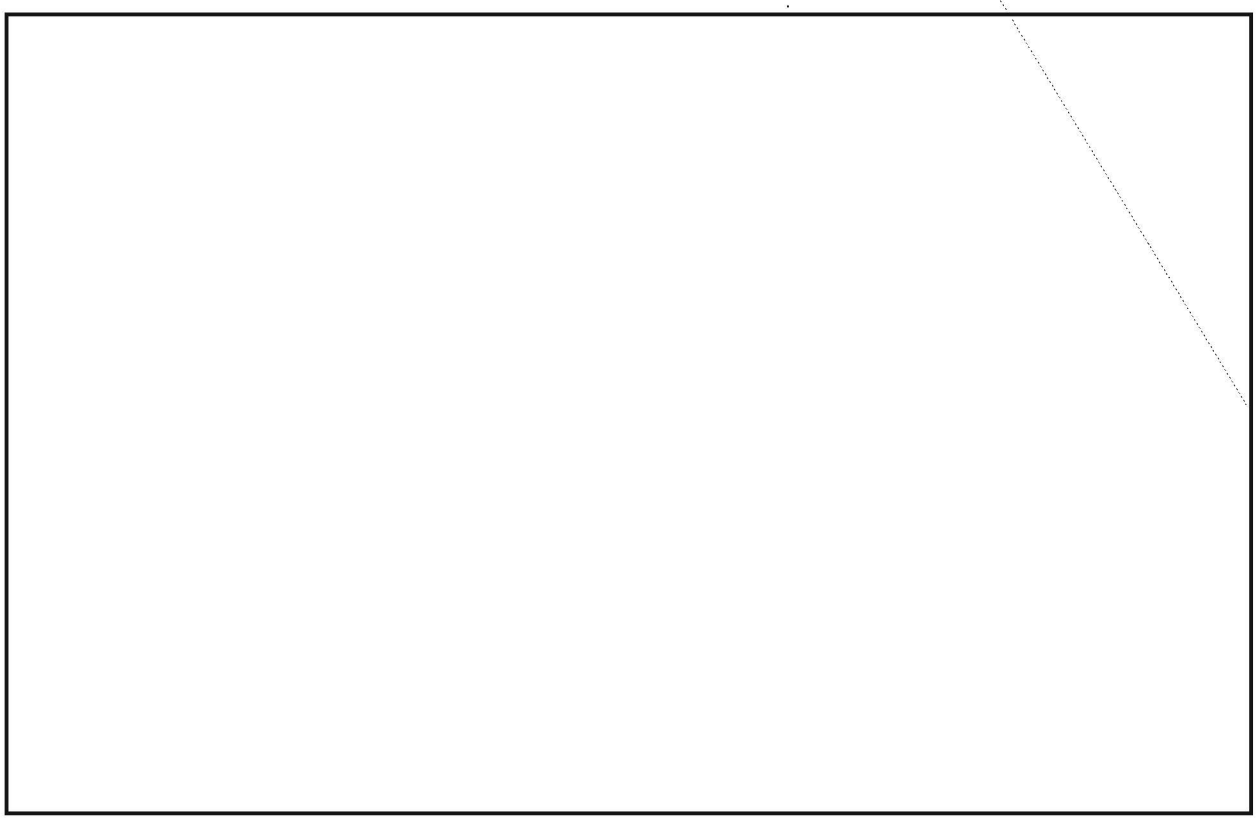
NOTE: The text of the quotation is classified CONFIDENTIAL - HVCCO.



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



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



~~TOP SECRET~~