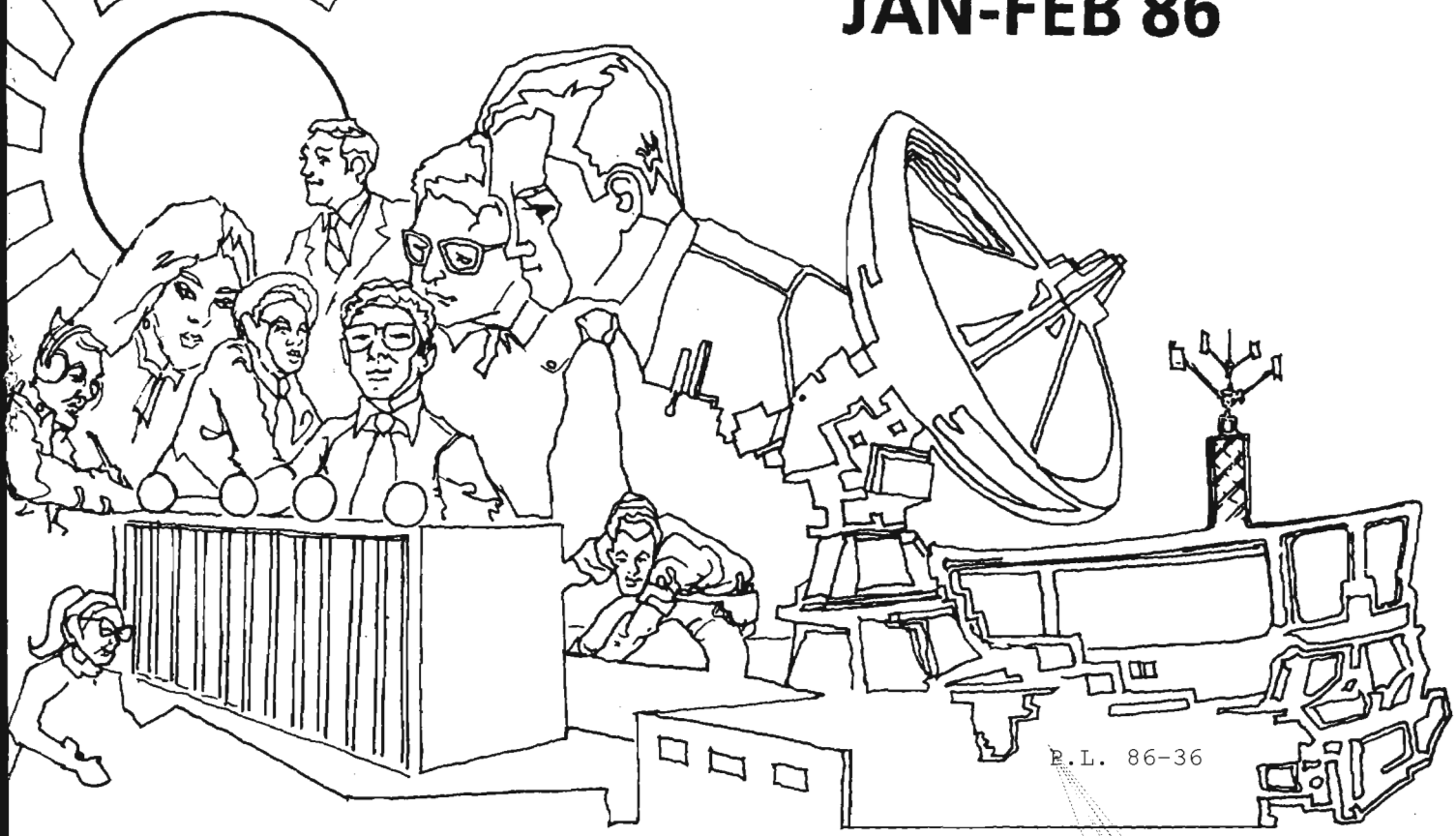
~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JAN-FEB 86



P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~
~~NOT RELEASABLE TO CONTRACTORS~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating Agency's Determination Required~~

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XIII, Nos. 1-2 ..... January-February 1986

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
cryptolg at bar1c05
(bar-one-c-zero-five)
(note: no 'o' in 'log')

Always include your full name, organization, and secure phone number.

For Change of Address
send name and old and new organizations to:
Editor, CRYPTOLOG, P1

HYDE PARK CORNER (u)

Readers sometimes hesitate when they mention an idea for an article because the subject might be "controversial" and therefore not suitable for CRYPTOLOG.

On the contrary!

*From its inception CRYPTOLOG was intended to be "informal, newsy, **controversial**, lively, and timely ... " If you read carefully some of the articles in this issue you will certainly find examples of controversy {DIFFERENCE OF OPINION}. If you leaf through back issues of CRYPTOLOG and of its predecessors you will sure find controversy {DISCUSSION, DISPUTE, DEBATE}. Especially in the Letters to the Editor you will find a notable instance or two of somewhat heated controversy {QUARREL, STRIFE}.*

For CRYPTOLOG is the analysts' own Hyde Park Corner. We actively solicit articles and letters on the hot topics of the day. We especially welcome comments -- the free and easy kind that analysts make around the coffee pot -- on articles that have been published. Open discussion, dispute and debate are absolutely vital for keeping things in perspective, as we function in an environment that is necessarily closed to the outside world.

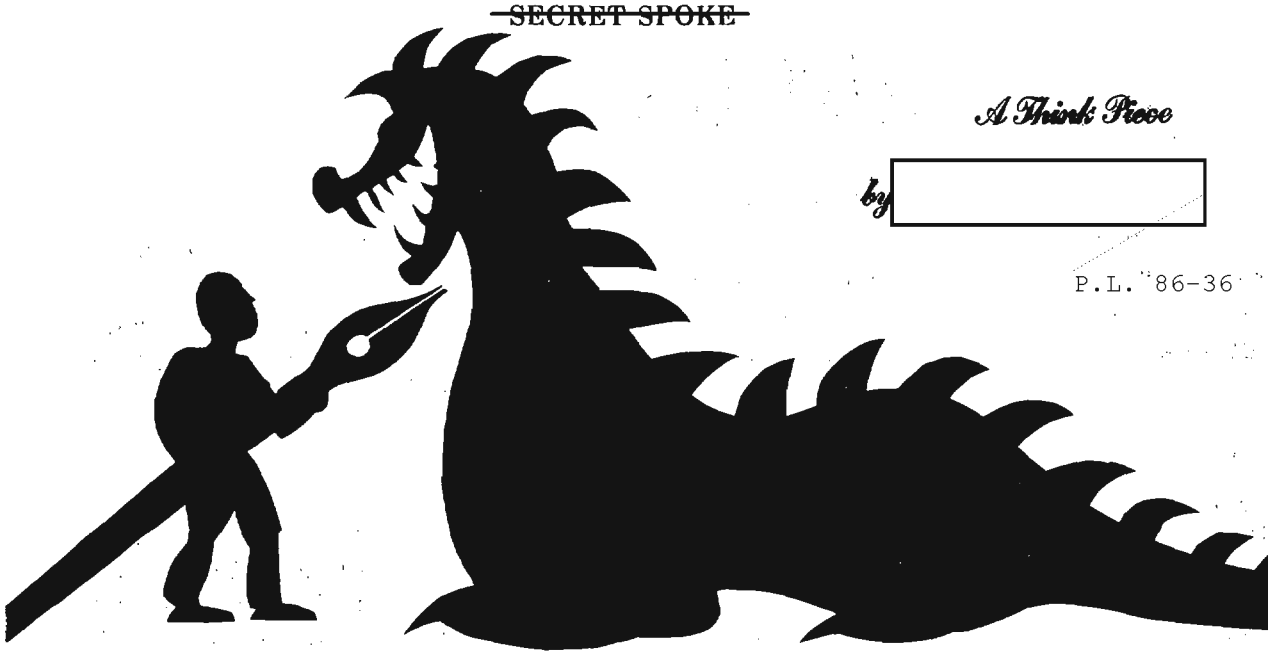
Among the "controversial" subjects that are frequently suggested is the relationship between NSA and contractors and vendors: how it affects what we do and the way we do it.

Another frequently mentioned subject is whether technical experts or generalist managers should make certain kinds of management decisions.

Now, when can we have that article ...

Ug

~~SECRET SPOKE~~



A Think Piece

by [redacted]

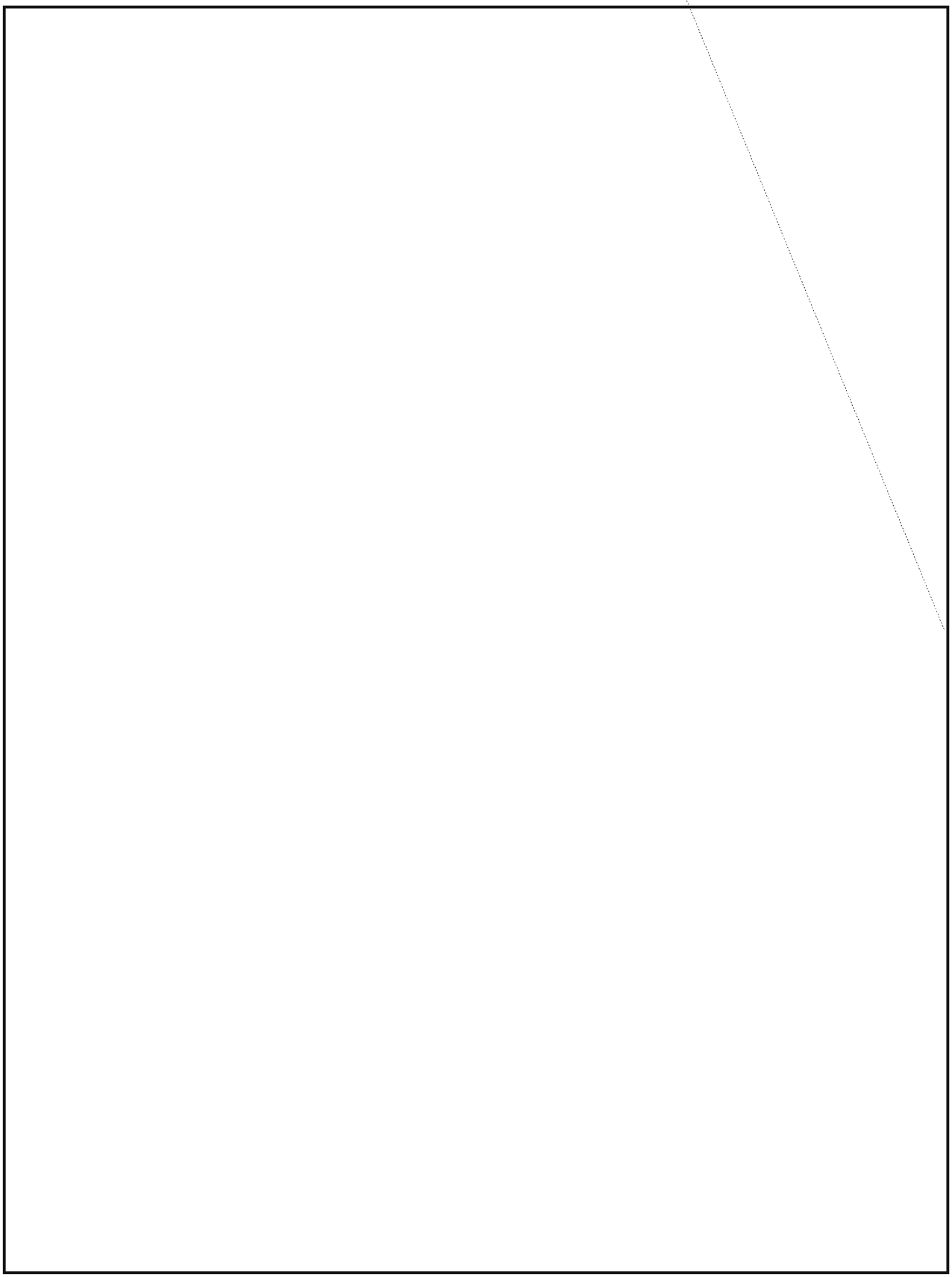
P.L. 86-36

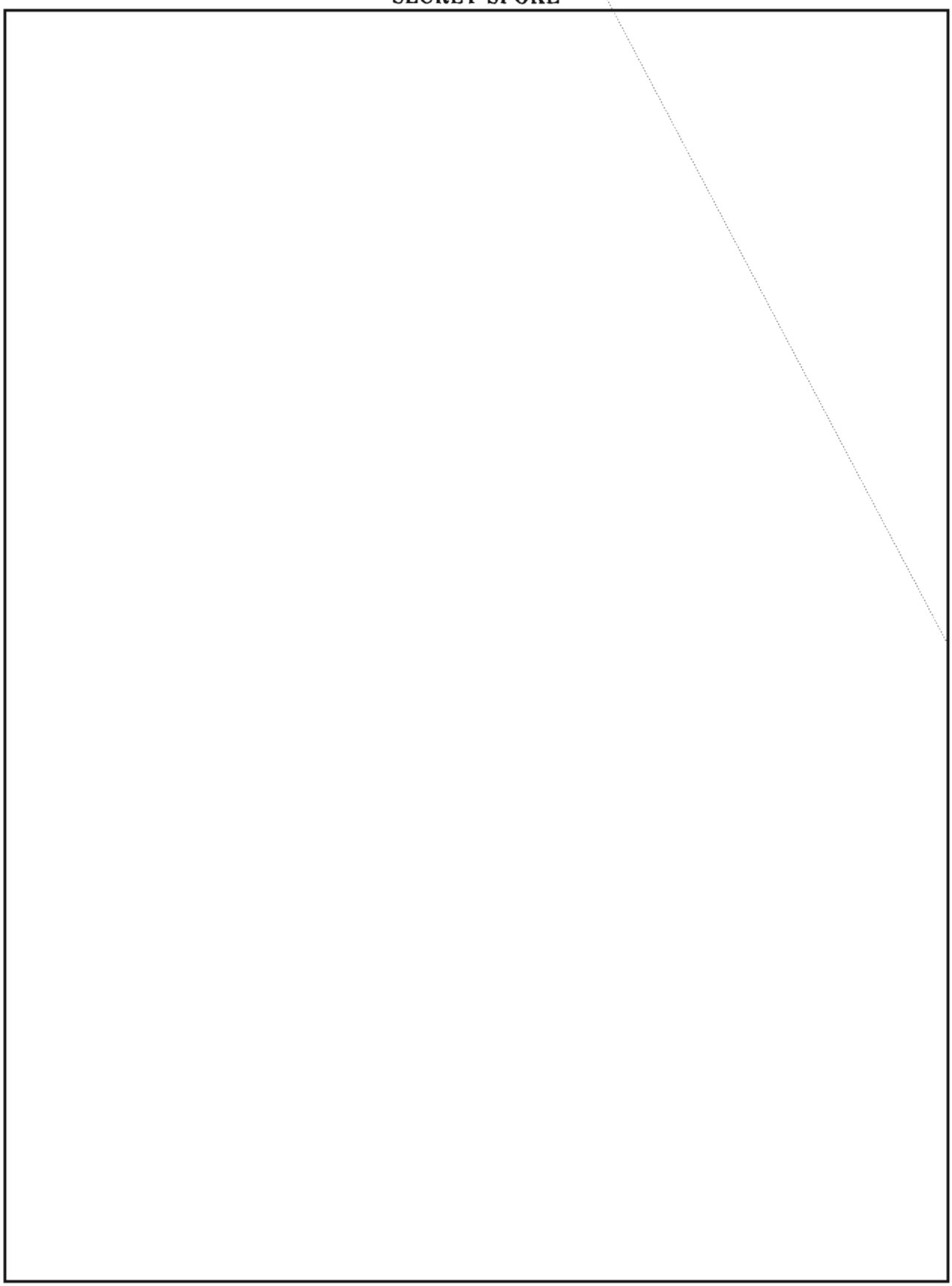
What I Perceive to be Happening in the Pacific (u)

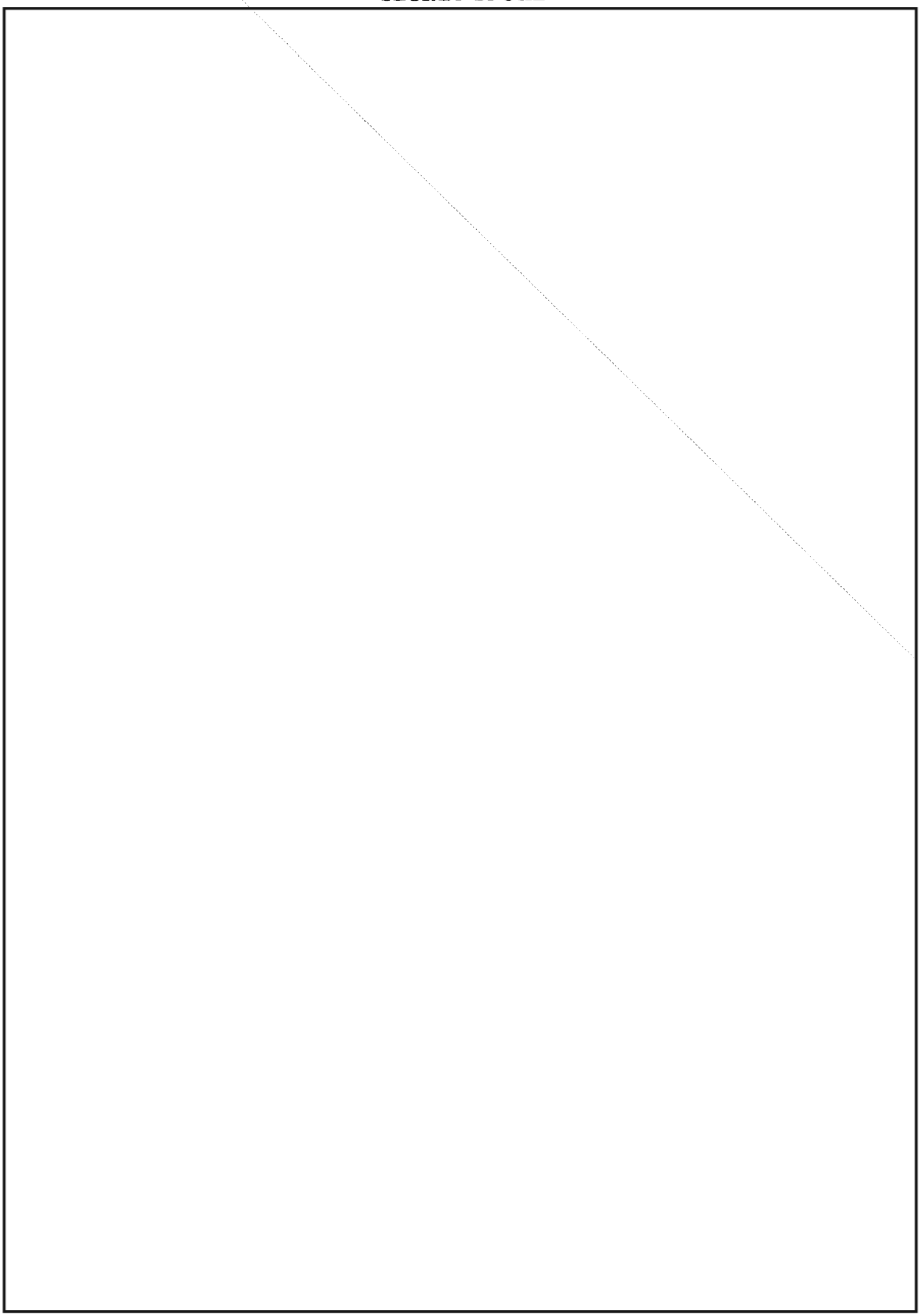
EO 1.4.(c)
P.L. 86-36

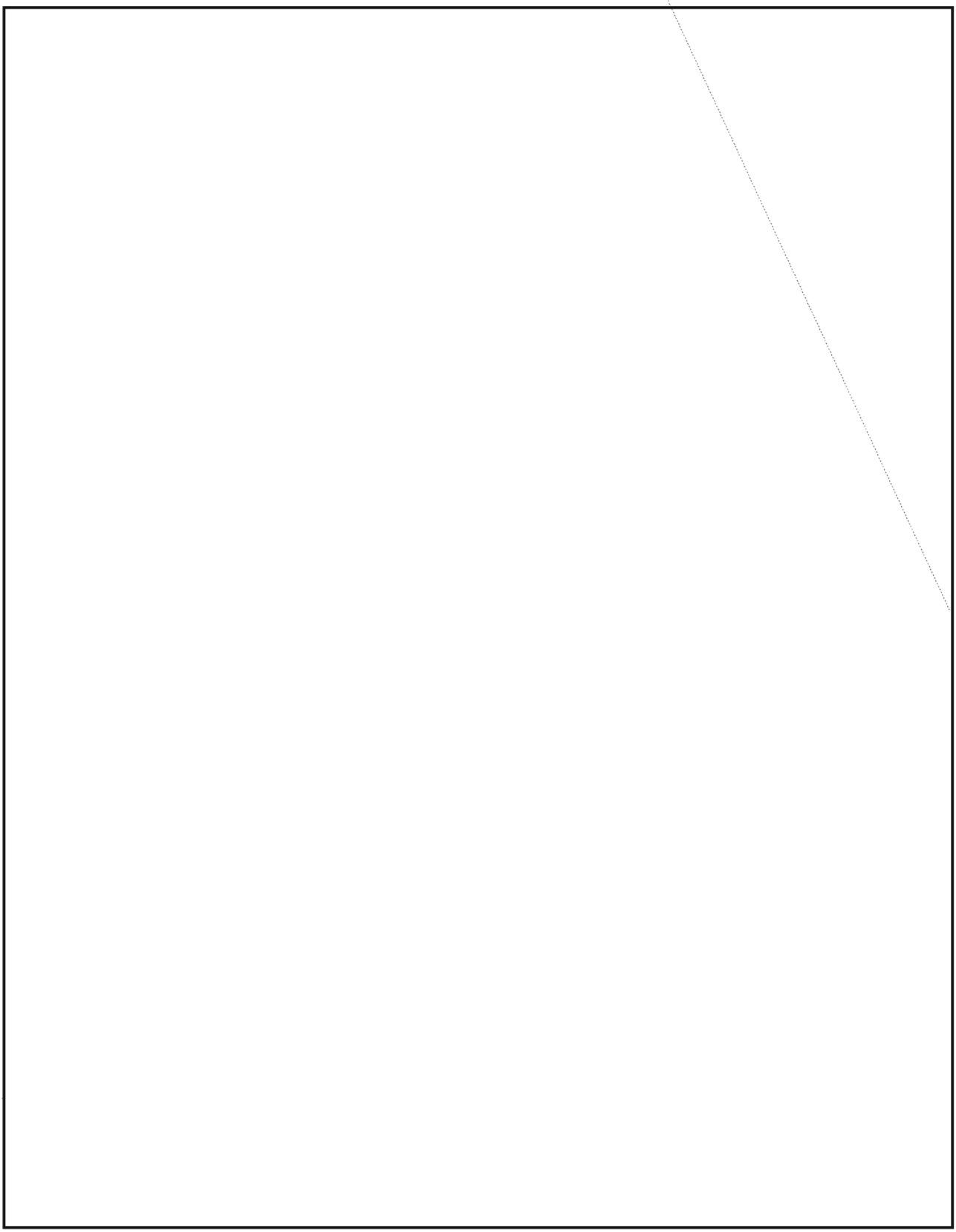
[redacted]

~~SECRET SPOKE~~









Diary of a Geisha (u)

E.O. 1.4.(c)
P.L. 86-36

P.L. 86-36

[redacted] *P56*

[redacted]

(U) The result was many, many meetings between reporters, programmers, and a patient group of interpreters on the G95 computer support staff who attempted to make sure each group knew what the other was talking about. Eventually a series of truths became self-evident:

▪ Preparation of product would take longer. Although it at first appeared incompatible with the goal of speed through computer automation, in fact using computers meant more work for the reporters. Speed and accuracy were gained by alleviating retyping of the item, and by easing the work of editors. But the time required to translate and prepare a product would be significantly longer, especially during the initial training period.

▪ Changes in the translating/report writing/editing sequence (i.e., the way we did our work) would be necessary. We would no longer be able to have two people working on one message at the same time and we could no longer casually pass a translation to someone for checking. We would be required to formalize our product preparation and release chain.

▪ People resist change. Back in the early days of PPREP, personal computers were rare and even the few existing enthusiasts were leery of a change that was going to slow down their work.

▪ We were going to do it anyway.

(U) Early on, it became clear that the software being used in G5 was not going to work for G9 and probably not for the rest of G Group. Being the first G office to go operational in a big way, G9 worked over a number of proposals and tried out a number of test programs. The general requirements as expressed to the programmers were:

▪ The system had to be non-technical, requiring only that users know how to operate the terminal. A knowledge of programming and sophisticated user techniques would not be necessary. In addition, instructions on using the system were to be integrated into the screen display so that the computer itself would move the user along, give him choices as to what to do next, point out errors, etc., and hopefully make it impossible for him to create a really serious problem. In programmer jargon, the system had to be user-friendly.

▪ The system had to be 95% error free before we would use it operationally. In addition, we had to have the ability to know where a given report was at all times until it left the building. We could not press the send button and just assume that the report had gone to the correct destination. As we were to learn, this didn't always happen. We

needed a system of receipt and the possibility of a complete audit trail for each product.

▪ Technical backup in the form of programming and hardware support had to be available at all times.

(U) We had many more requirements, some technical and some intended to limit the computer burden being placed on the analysts. But the point we kept hammering home was that the product had to get out and that timeliness and accountability were essential.

~~(FOUO)~~ As we looked to the future we identified two major tasks. The first was to come up with a good, reliable system. The second was to figure out how we were going to get hundreds of diehard pencil pushers and blue pencil editors to sit at a computer terminal and use the system that was developed. Hard though it is to remember now, as late as 1983 linguists and reporters still functioned in a totally paper world. We had access to SOLIS and a few other computer-age aids, but the tools of our trade were the yellow legal pad, carbon translation forms, and the much hated G-Group Expert sheet for technical accountability. In many ways this was a comfortable method of operation, reminiscent of our days in academia when we were tucked away with dictionaries and reference volumes, busily filling reams of paper.

BEFORE PPREP

~~(C-CCO)~~ In those Days of Olde, translators selected an item to report and wrote out a translation. If they made a mistake they crossed out or erased and, when they needed help, they took the translation to another linguist for consultation. When the translation was completed, both the text and the translation were placed into a checker's bin for review. When the checker had finished, the translation and text were placed back on the preparer's desk for correction and revision. Sometimes the whole translation/checking process had to be repeated several times.

~~(C-CCO)~~ When the translation was approved, the decision was then made as to whether the item would be published in full-text translation format or as a gist. Finally, the preparer was responsible for completing the EXPERT sheet, filling in the report title, TAG line, requirements, collectors, times of intercept, links, lanes, mat numbers, case notations, worksheet numbers, serial numbers, languages, etc. etc. etc. for the traffic used in preparing the report. Then, the finished product package, usually made up of at least three copies of the report and five copies of the Expert sheet, was placed in a supervisor's bin for review.

~~(C-CCO)~~ The supervisor edited the product and usually passed it on to the branch level for further review. The branch chief then passed the package to the people responsible for assigning the correct product distributions, DDIs, etc. The product was

(U) All of this may sound cumbersome, but it was the system we knew and loved and we were loath to give it up. At least it worked.

CHANGES

~~(FOUO)~~ Obviously, many things had to be changed as we moved to computers. We had nowhere near the number of terminals required for the number of reporters/linguists who needed to use the system. In addition, you could not casually pass a computer screen back and forth to a checker, nor could you allow everyone to release product to NSOC without control. Following a lot of talk and a lot of compromises, a number of procedures were developed:

- Reporters were not to take the place of the FLEX pool. By that was meant that we would not carry on as before, preparing translations and reports on paper and then once they were approved, retyping them into the computer as FLEX had been doing. Rather, analysts would work directly on the computer from step one. As more terminals became available, more reporters would use them. Any given report, however, would either be prepared and processed using the computer route or the paper route, no mixing of the two.

- A chain of logins with limited sending authority would be developed. Linguists would be able to send a report for checking to anyone in their login, and could then get it back again. The finished report could be sent only to an authorized login. This restriction extended up the editing chain as the product package was prepared for release; it was intended to minimize the risk of losing product through careless typing. Although there developed individual variations within offices, usually a product went from preparer, to checker, to branch, to distribution, and finally to NSOC, where it became that element's problem to dispatch product to the recipients.

- Distribution personnel within each division were made responsible for ensuring that product was not lost enroute to NSOC. This was done through use of a system of PPREP report numbers and a system of receipts generated by the various computer systems sending and receiving the reports.

- Training of personnel and operational use of the system would be very carefully controlled and instituted very slowly. Training was obviously one of our biggest headaches. Once we had a fairly workable system we had to ensure that people knew how to use it properly. Yet we also knew that the system would change frequently, particularly in the early months, and we had to have some mechanism for quickly disseminating information about changes in procedures or system usage.

TRAINING

(U) What evolved was a training strategy based on the pyramid. Initially a small team of fewer than ten people was formed, consisting of two people from each of the G9 reporting divisions. This group formed a steering committee and was fully indoctrinated into the system both technically and emotionally. That is, not only were they to learn the system inside and out, but hopefully they would like using the computer and drum up a little enthusiasm among their more reluctant co-workers. Once this initial group was trained, these people became responsible for training other people in their division, who were made responsible for training others, etc.

(U) Information on changes in the use of the system was passed downward the same way. The main advantage of this system was that we had to train formally only a small group of people, thus lessening the burden on the steering committee whose members, after all, were linguists and reporters with other responsibilities.

~~(FOUO)~~ The actual training involved the preparation of a number of G9 working aids among them:

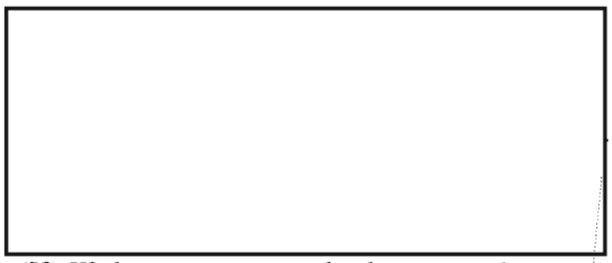
- "PPREP Users' Guide," which tried to include everything known about PPREP operations;

- "PPREP Users' Instructions Quick Reference," which gave step by step instructions for logging in and making the appropriate screens appear;

P.L. 86-36

(U) The prospective user was first presented with the fifty-some pages of instructions as a security blanket, told to skim through this documentation, and then then swiftly brought over to the terminal itself for the all-important hands-on training. After several magic shows in which the razzle dazzle of the computer was displayed, the students quickly settled down to discover that they had to use the system in order to learn it.

STARTING OUT



(U) We began very, very slowly--two products a day to start. If we had trouble one day we tried only one product the next day. We tracked each product through the system and checked the DDP feedbacks very carefully. To say that we had problems would be an understatement: we had trouble getting receipts, product was lost "somewhere," extraneous letters appeared in TAG lines, lines of text disappeared, we had product that the computer simply would not forward although we couldn't find any errors. One day we issued what turned out to be utter gibberish--the computer had taken a tabular report and forced it into paragraphs resulting in unreadable nonsense.

(~~FOUO~~) We made progress. With constant support from the programmers in T3 we gradually increased the number of products prepared and released via PPREP each day. By December, we had achieved such success that we decided it was safe to expand the training and operational use of the computer to the three other G9 reporting divisions. We gained an additional terminal subsystem (TSS) which, of course, caused a whole set of new problems. But within six weeks all four reporting divisions were using the computer. In January 1984, G9 was producing 5.3% of its product on [redacted]; in March it was producing 15%, in April 30 percent, and by June, G9 was producing 52% of its product on [redacted]. Product review items can now be prepared and released via PPREP.

(U) PPREP has become a way of life for G9ers. Most junior linguists continue to do paper and pencil translations which they have had checked and then bring to the computer to prepare a gist. Words like NROFF and ARG BREAK and PICKING and PUTTING are bandied about as product is prepared and preformatted expert sheets with prefilled standard fields are completed. Word is passed to editors when they have product in their "mailbox" and distribution personnel check technical details before pushing the button that sends the product to NSOC. The number of available terminals has gradually increased as has our dependence upon them. Many people find that they actually write better on the terminal than on paper because of the ease of self-editing.

(U) During system outages, which occur, alas, all too frequently, albeit (usually) for not too lengthy a period, most analysts find something else to do, leaving report preparation for when the system comes back up. During a recent extended outage when we had to get product out, my section first had to resurrect some typewriters from atop file cabinets. Major problems occurred when we tried to remember how paper Expert sheets were supposed to be filled out and how many copies of everything were required.

(U) Is PPREP a success? Most analysts will say yes. Are there still problems? Yes. There are major headaches and minor inconveniences but in the main, the lot of the linguist/reporter has improved and continues to do so because of the computer system and the programmers who patiently support us.

(U) Recently G9 began to receive the Agency Standard Terminal Workstations, a/k/a ASTWs. The terminal works as a stand-alone computer but can also connect to the GEISHA system to be used for product preparation. One set of key functions is written on a plastic overlay that surrounds the keyboard; we use those key functions when the terminal is being used in the GEISHA mode. Another set of key functions is posted on a keyboard diagram attached to the side of the terminal; this applies (mostly) when the terminal is being used as a stand-alone. (A third set of functions keys we ignore; the standard keyboard issued from the manufacturer contains keys which have not been enabled.) There is also a "forbidden key" in the stand-alone mode which turns everything into what resembles irreversible hieroglyphics

P.L. 86-36

POSTSCRIPT

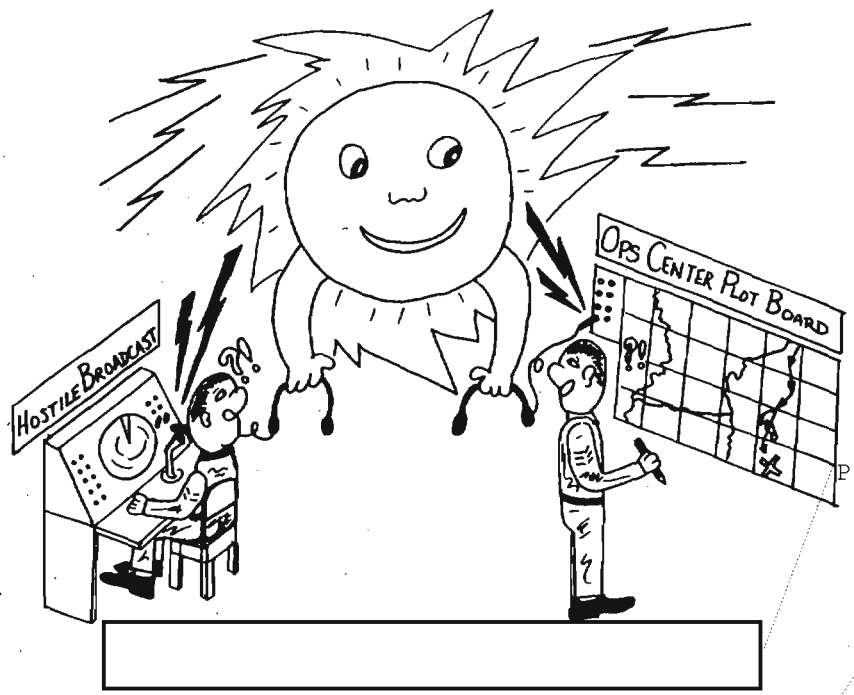
(U) My technical mentor tells me that the Forbidden Key problem has been solved with new software. However, just the other day my office got a new ASTW, and as I struggled to load it I accidentally pressed that key! I shouldn't have... □

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

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

P.L. 86-36

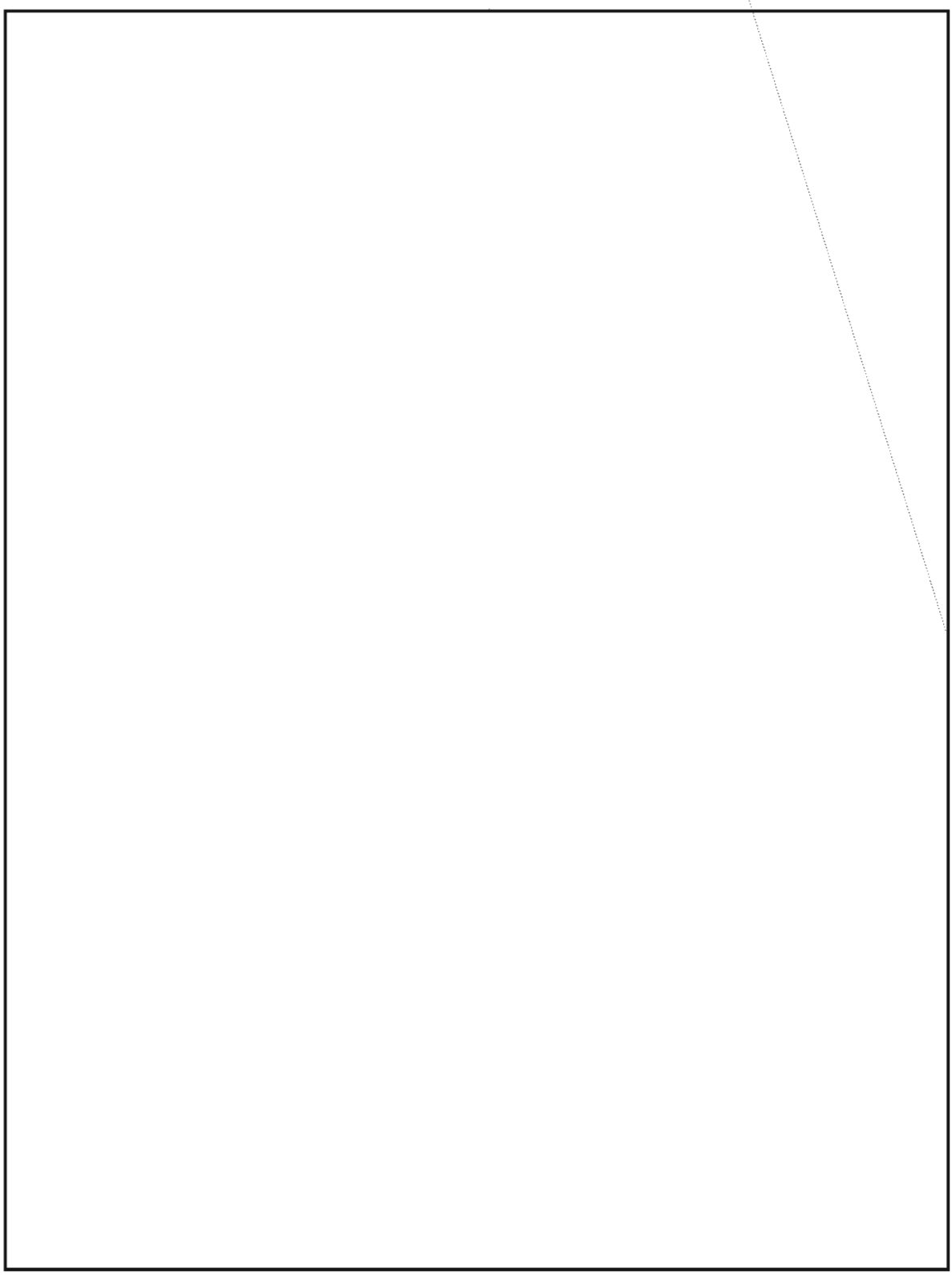
A CASE OF FORENSIC SIGINT (u)

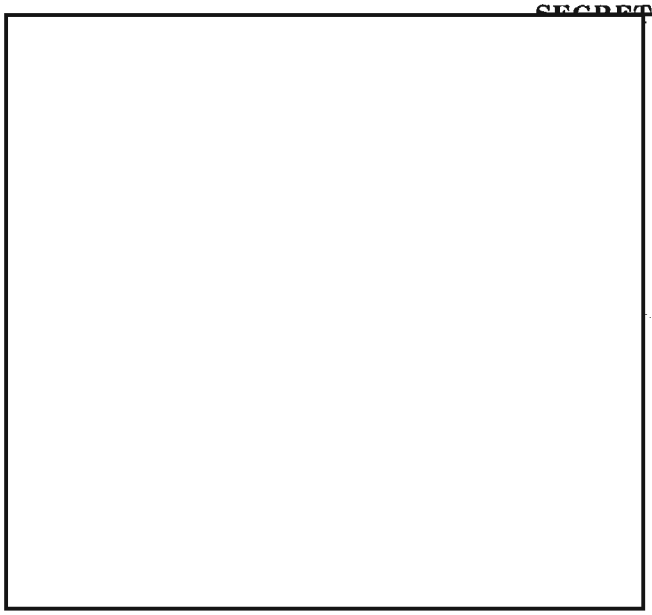


EO 1.4.(c)
P.L. 86-36 P.L. 86-36

(U) SUNSPOTS???

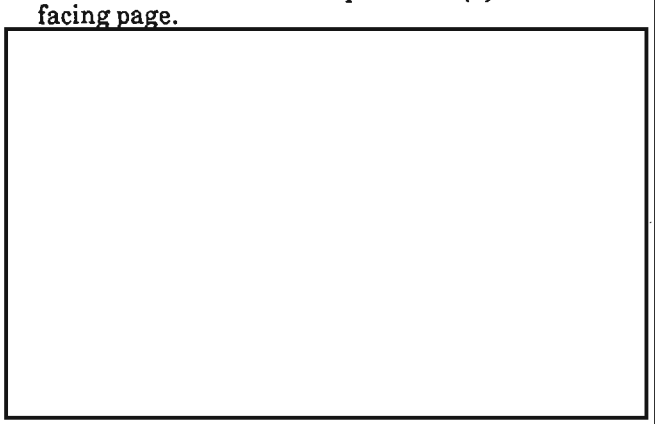
~~(FOUO)~~ While I knew that our colleagues would find our explanation of what had just happened hard to believe, the reaction was even stronger than I had anticipated. But the first explanation of the event had been just too simple to be correct. On top of that, it didn't square with the target's mode of operation. There had to be another answer, and it had to be atmospheric in origin.

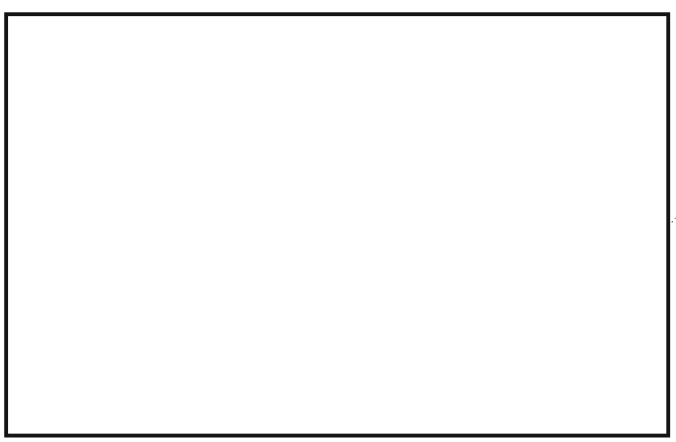




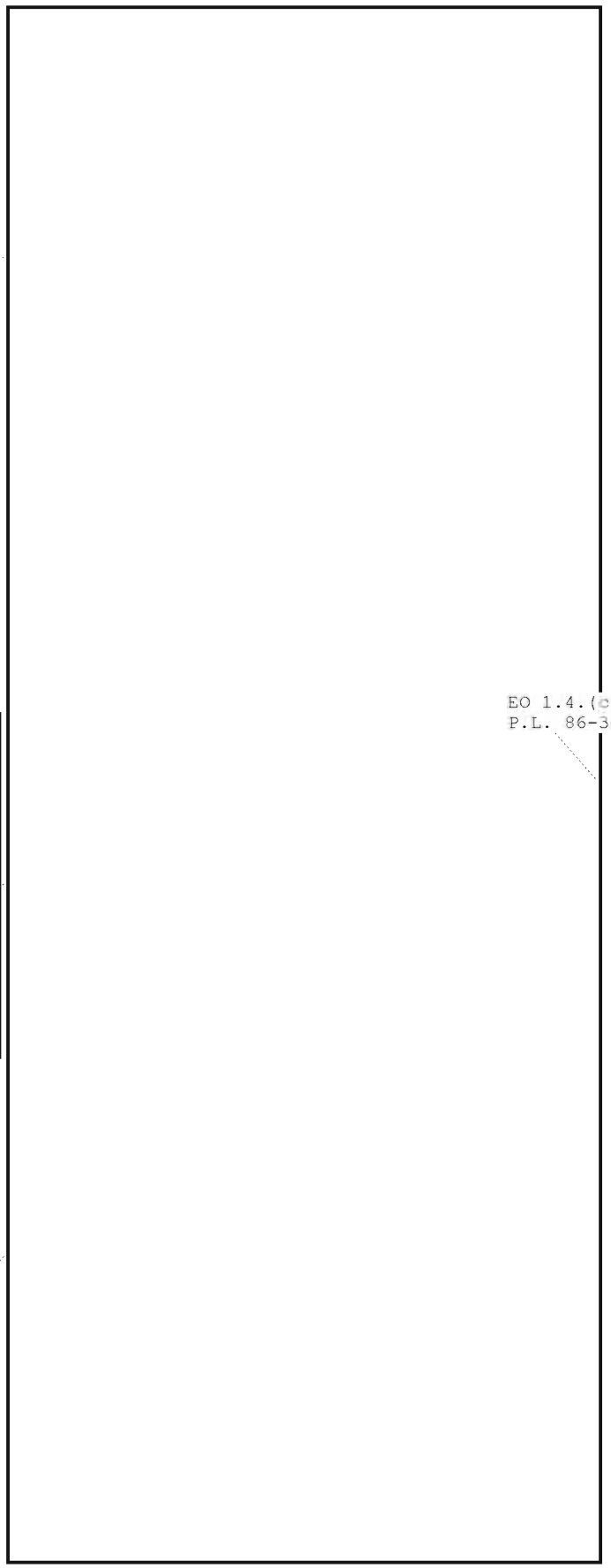
(U) As luck would have it, Murphy's Law was operative on that day. A US field station in the vicinity issued the SPOT report marked {1} on the facing page.

(U) Approximately one hour later, the same station issued the follow-up marked {2} on the facing page.

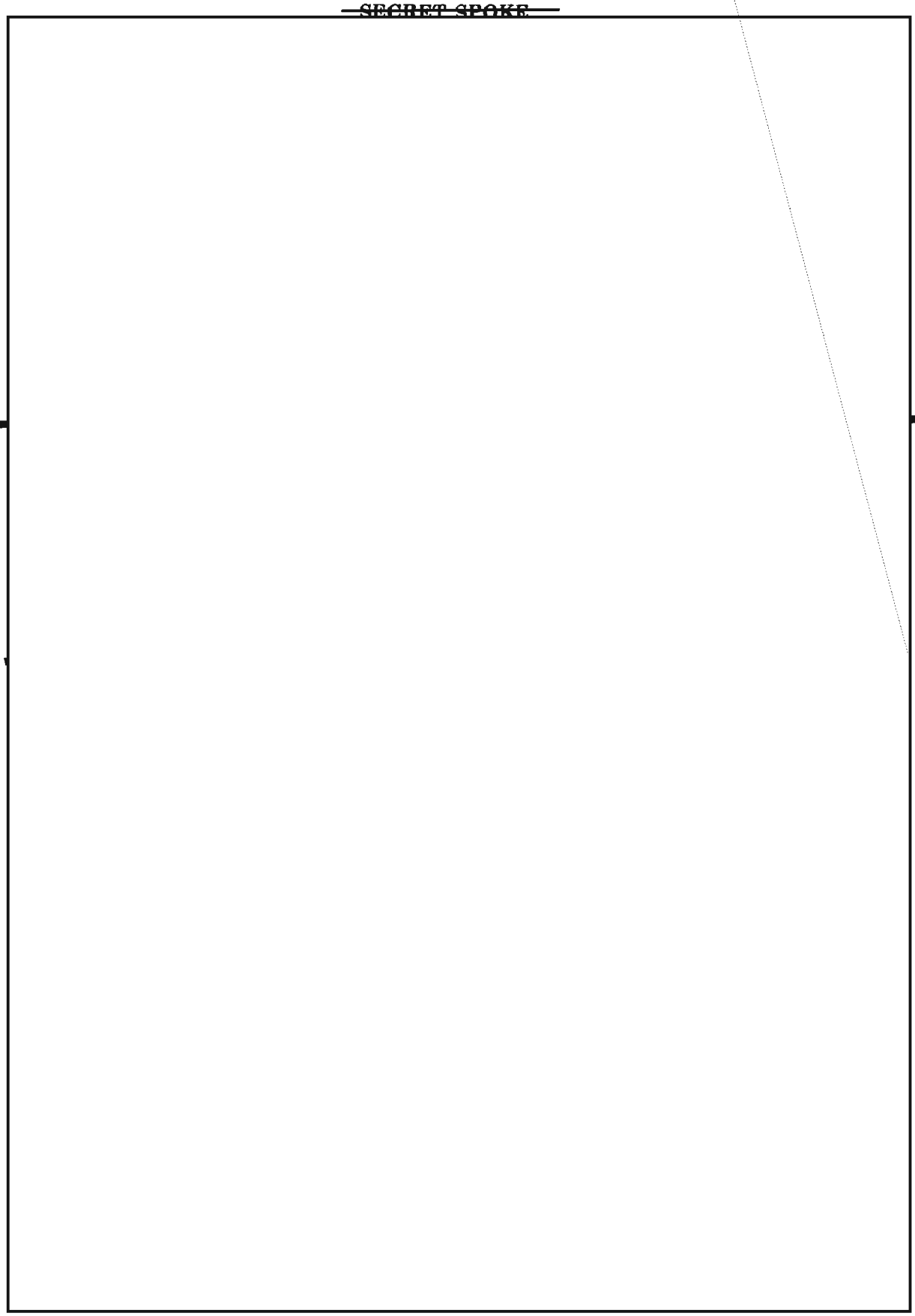




~~(S)~~ This indicated to our analysts that the answer lay not in willful suppression of tracking, but inability to communicate. What was the cause, then? Jamming? That was not considered a



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



[redacted]

Ed,

Your question prompted me to do some more homework on solar flares. In the NSA library I found a book titled Solar Flares *by Smith and Smith (McMillan, 1963).*

Pages 242-250 describe the sudden ionospheric disturbances (SID) accompanying some solar flares and consequent short wave fadeout (SWF) alluded to in our report.

According to Smith and Smith, SID is noted "only in the illuminated hemisphere" and occurs simultaneously with the event. "This class of terrestrial response must therefore be due to short-wave electromagnetic radiation of the flare." (p. 242.)

"SWF are the most familiar and certainly the most economically significant ionospheric flare effects ... Fadeout may become complete in as short a time as one minute, and can endure from a few minutes to several hours." (p. 243.)

"An ionospheric disturbance characteristically begins about 7 minutes after the flare commences, but this time is always during the flare's rise to maximum." (p. 244.)

"We mentioned earlier the observed time delay between maxium phases of flare and SID [7 minutes]. Some authors have pointed out that the delay can be interpreted simply in terms of the normal response of ionsopheric layers to an impulsive rise in the flux of ionizing radiation. Thus there is no need to assume that in the rising stage of a flare, there is time sparation between its visible and its ionizing radiations." (p. 249.)

[redacted]

CRYSCO - 86

THIRD ANNUAL CONFERENCE

2 - 6 June at NSA

Sessions held in the Friedman Auditorium
and in Conference Room 2W087

AUDITORIUM SESSIONS ARE OPEN
to persons with green or orange badges

OTHER SESSIONS REQUIRE TICKETS
(distributed through your office)
a green or orange badge
and LACONIC access.

Topics for the conference room sessions include:

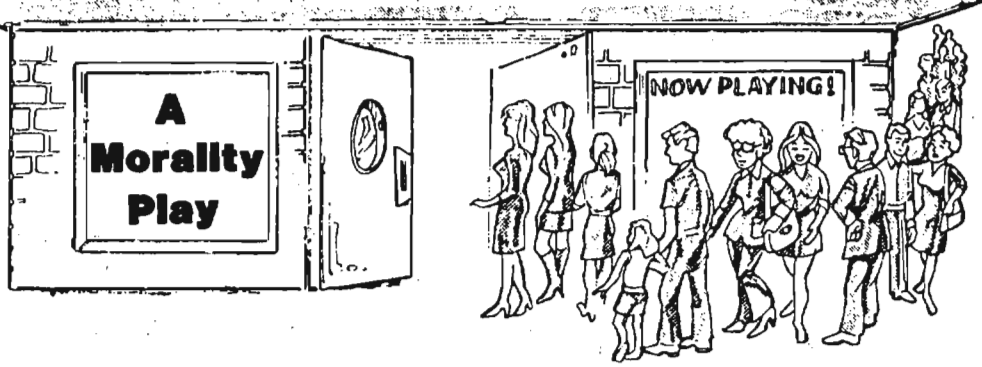
- HYPERCAN hardware, present and future;
- CRYSCOs in review;
- Components of distributed processing;
- Cryptanalysis on personal computers;
- Life after IMP;
- Software exchange -- can it work?
- Major applications packages;
- Parallel computers and their applications;
- Automatic processing packages;
- Diarization packages;
- Computer graphics for cryptanalysis;
- CRYSCO-86 wrap-up.

Additional information can be obtained from the CRYSCOM Executive [redacted] *A531/P13, 963-3197s.*
(FOUO)

P.L. 86-36

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

HOW 25-5 REALLY WORKS



HOW 25-5 REALLY WORKS

A MORALITY PLAY IN ONE ACT

BOOK

by [redacted] N34

Adapted for the Stage

by [redacted] *T091*

and [redacted] *T091*

Sets and Costumes

by [redacted] *B54*

★ *A Va Production* ★

★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★

DRAMATIS PERSONÆ

in order of appearance

Fred Finder, a DDO analyst

Heinous Merger, his boss

Tom Talker, an N34 budgeteer

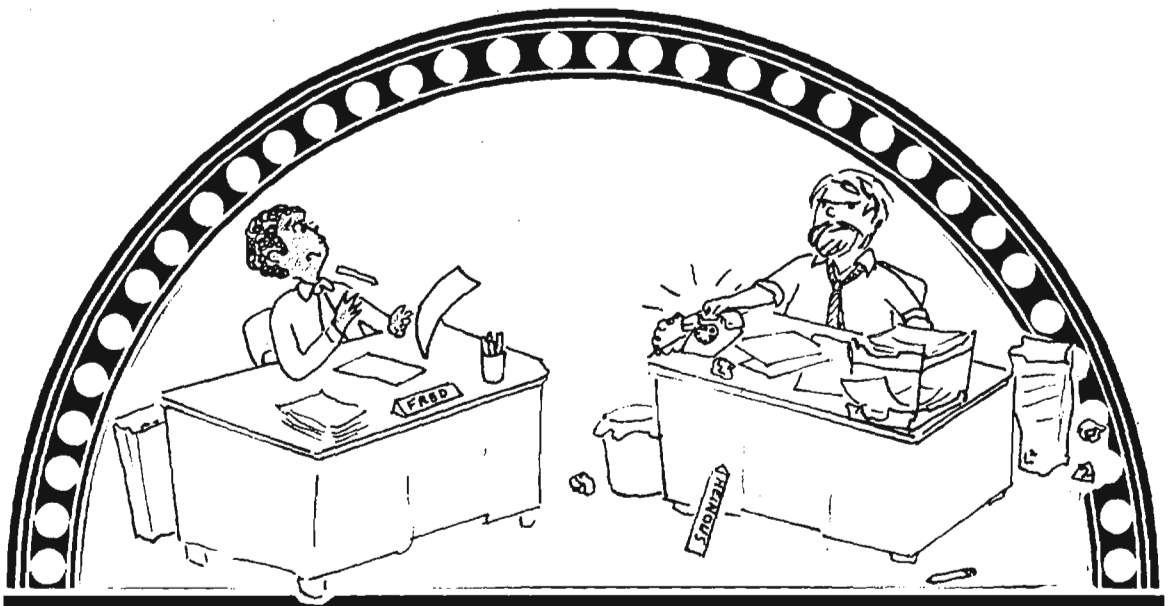
Rosa Really, his boss

★

The action takes place at NSA

★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★ ★

P.L. 86-36



Scene 1

Heinous Merger's office in a DDO element.

Don Dillman runs a free wheeling R&D Shop and had been building "black boxes" for Heinous. Everything had worked well until he and Heinous dreamed up RATTLECAN. Heinous did not have any problem getting the funding into the outyear program, but the cost and the wide deployment of the RATTLECAN asymmetric permutated muxes (APMs) attracted attention in N34.

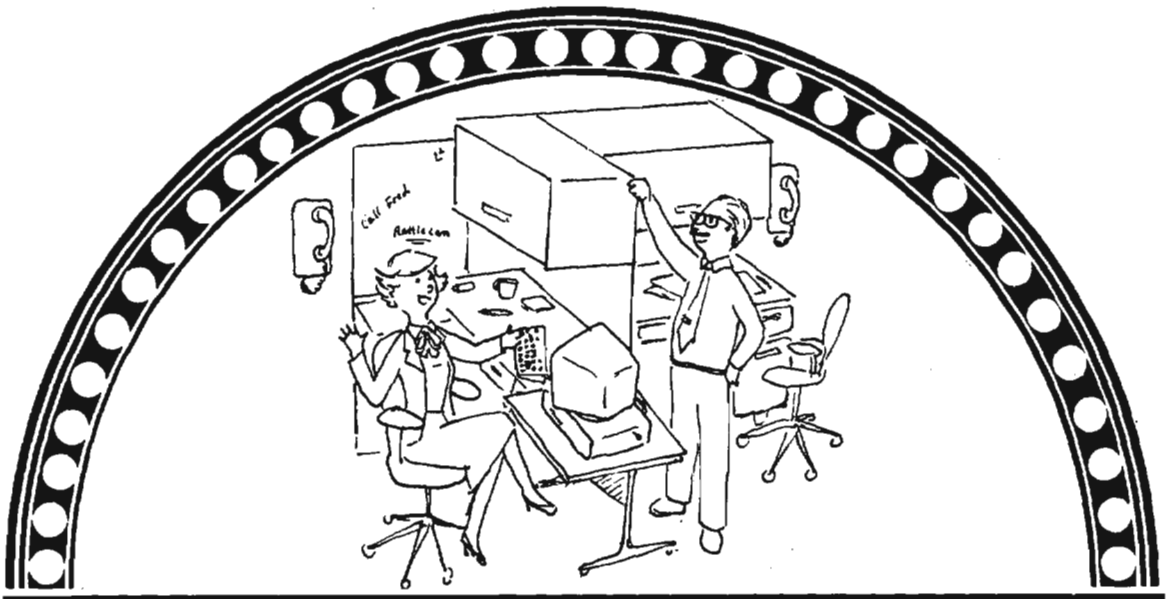
As Heinous crashes the phone into its cradle, Fred jumps.

Fred: Take it easy on the phone, Heinous ... it's not MILSPEC.

Heinous: #$%&*@! That nerd Tom Talker in N34 took the RATTLECAN money out of the program build.

Fred: I've tried to tell you, Heinous, you can't duck the regs forever. Sooner or later you've got to document RATTLECAN.

Heinous: I don't see why, Fred. I got my money in the budget and I know what I want to do. Don Dillman's shop has been working with those APMs and they'll be just the thing to get this signal.



Scene 2: Rosa Really`s office in N34

Tom: Rosa, I think that we ought to bring RATTLECAN under NSA/CSS Circular 25-5.

Rosa: Why?

Tom: First, the project clearly falls under 25-5 because of the cost, $11M.

Rosa: I know that, but do we really need 25-5 monitoring for an off-the-shelf buy like this? Isn't Dillman's shop just going to use a bunch of APMs?

Tom: Yes. They have worked well in stand-alone applications, but a network of them could be a considerable risk. There may be a better way.

Rosa: Well, what should we do?

Tom: I think that, considering the cost, the potential risk, and the widespread use, a few other organizations need to look at RATTLECAN, and corporate management needs a say also.

Rosa: I certainly can't argue with that rationale, Tom. That's what 25-5 is all about. Send a memo to DDO reminding them that they need to get their RATTLECAN documentation in by 1 March if they want to get into the FY88 program build.

Scene 3: Same as Scene 1.

H [screaming]: I haven't written a 25-5 requirements paper yet and I don't intend to start now!

F: Oh yeah, How are we going to get the money for RATTLECAN without one?

H: Oh @#$*! What do we do now, Fred? I've spent my whole career ducking 25-5.

F: It can't be as bad as all that. Lots of people have done it. A classmate of mine from the War College is in N342 now; maybe she can help us.

A few minutes later.

Rosa enters stage right with Tom.

F: Hi, Rosa it's good to see you again. Thanks for coming over. Meet, Heinous Merger, my boss.

H: Hello Rosa, my friends call me Heinous the Hutt but you can call me Heinous. How can you stand all that paper shuffling Rosa? When are you going to start producing some SIGINT like we're paid to?

R. Let me explain a few things. The 25-5 process has some good and proper goals. It gives the project sponsor high-level visibility and corporate support; it gives the Agency seniors a mechanism to review acquisition initiatives; it gives the acquisition organization a bounded task; and, it provides an established procedure for project coordination. Everyone should understand what it's all about and know how to use it.

H: Sounds like baloney to me!

R: Tell me Heinous, do you think that you and Don Dillman should have free rein with the $11M for RATTLECAN? Don't you think that there is an off chance that someone else might have some useful information to add? Don't you think that the corporate management is entitled to some say in how money is spent? And what about the SCE's that will have to train people to operate and maintain the RATTLECAN gear, shouldn't they get a warning of what's coming?

H: Well, sure, in fact, I ran into the Director on the elevator yesterday and I told him all about RATTLECAN. He said to keep charging.

R: Is that the way we inform our corporate management, Heinous, on the elevator? Do you remember exactly what you told him?

H: Well, not exactly.

R: That's my point, Heinous. If we are going to run an Agency this big, many people have to know what others are doing. 25-5 is the way we make that happen.

H: I never thought about it that way. I guess the seniors do need a cut in here somewhere but I don't have to worry about communicating with DDR. My buddy in R, Don Dillman is a wiz. If it's SIGINT, he can make it.

R: Well, Don Dillman isn't the only engineer in R. There is another R office that's doing almost the same thing that you want to do with AMPs, only using massed digital modulators.

H: I don't care. I know Dillman and he can deliver.

R: Maybe so, but the MDM is the new agency standard for this type of collection. Integrating RATTLECAN into the MDM architecture will improve interoperability, lower costs, and improve maintenance.

H: Well, maybe so, but why do we have to get this stuff in so early? It seems like I just thought up RATTLECAN and the next thing I know I get a memo asking for a ton of paper.

R: There are many people involved in the 25-5 process. If things get dragged out at any one point it holds up everything else. You need to get started as soon as possible.

Rosa stands up and draws the chart shown on facing page

R: If we're going to have smooth acquisition planning, people have to do their parts on time or they'll mess up the people on the next link of the chain.

H: Boy this is bureaucratic, Rosa. Do we have to go through all this to get a system fielded?

R: Not always. The chart shows a situation in which all the steps of the 25-5 process are applied. In many situations, we modify the process considerably. We use only those steps that are appropriate to the action at hand. For minor systems you can use the PBS -- the Project Baseline Summary -- instead of the SCP route.

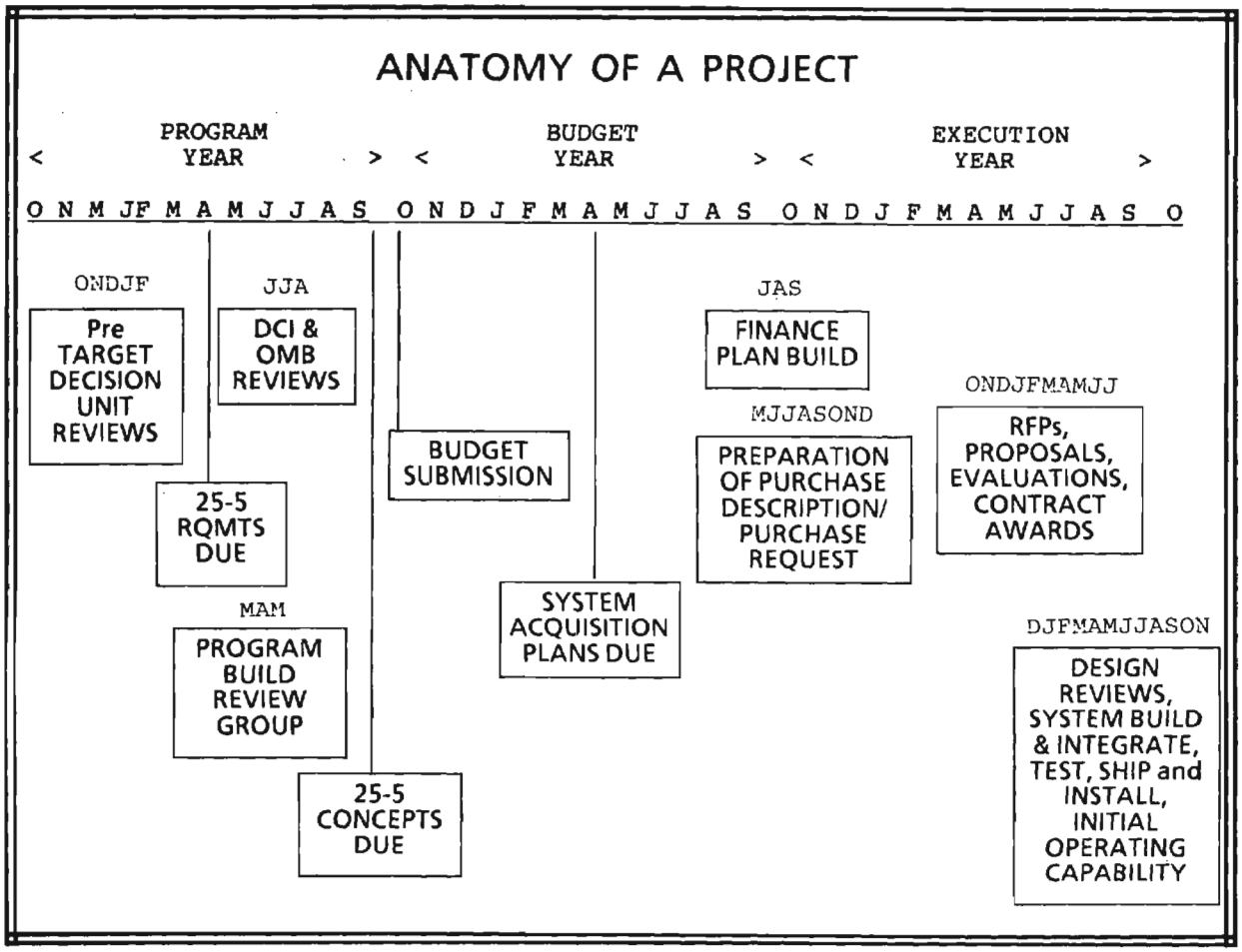
H: Gee, you mean we might not always have to do a SCP-III?

R: That's right. There are some times that it may be more appropriate to move straight from the requirement to the SAP. It all depends on the circumstances.

H: OK, but why all the big sweat about getting all this planning done so fast? After all we have three years to spend procurement money.

R: That's true, on a project basis, but things don't work that easily for the Director.

H: What do you mean?



R: Every year the Director and other Agency seniors go to Congress and defend our budget. They look pretty foolish asking for a big pile of money for the new fiscal year when they haven't even spent the money that was available in an earlier year. Also, if we don't spend the money on time, we lose millions of dollars a year just to inflation.

H: So the aim is to spend the money on what we asked for when we said we would need it.

R: Yes, plan your work and work your plan!

H: I'm convinced, Fred. Start up the boilerplate factory so we can get Ms. Really her requirement.

R: Thank you, but I hate to read boilerplate even more than you hate to write it. You don't have to rejustify your projects in the 25-5 documentation. All you have to do is describe them. We prefer clarity to volume. Six pages is the PBS goal, and two or three should suffice for a PBS Section I.

H: Six pages! Are you kidding?

R: No. SCPs of necessity will be longer but we don't pay for them by the pound, either.

H: Gee, Rosa, how do you know all of this anyway?

R: In N34 we review all the 25-5 documentation and it enables us to act as an "honest broker" for actions like the RATTLECAN. We're in business to make the 25-5 process go as smoothly as possible. Our system management officers all have considerable DDO, DDT or DDR experience. They can help you with all facets of 25-5 from writing PBS-Is to coordinationg SAPs. If we don't know the answers we'll find them for you. There are a lot of people who contact us before they even start a project. That way we can start greasing the skids for the project before it's even in the starting blocks. If you like we can set up a briefing for your people on the whole process.

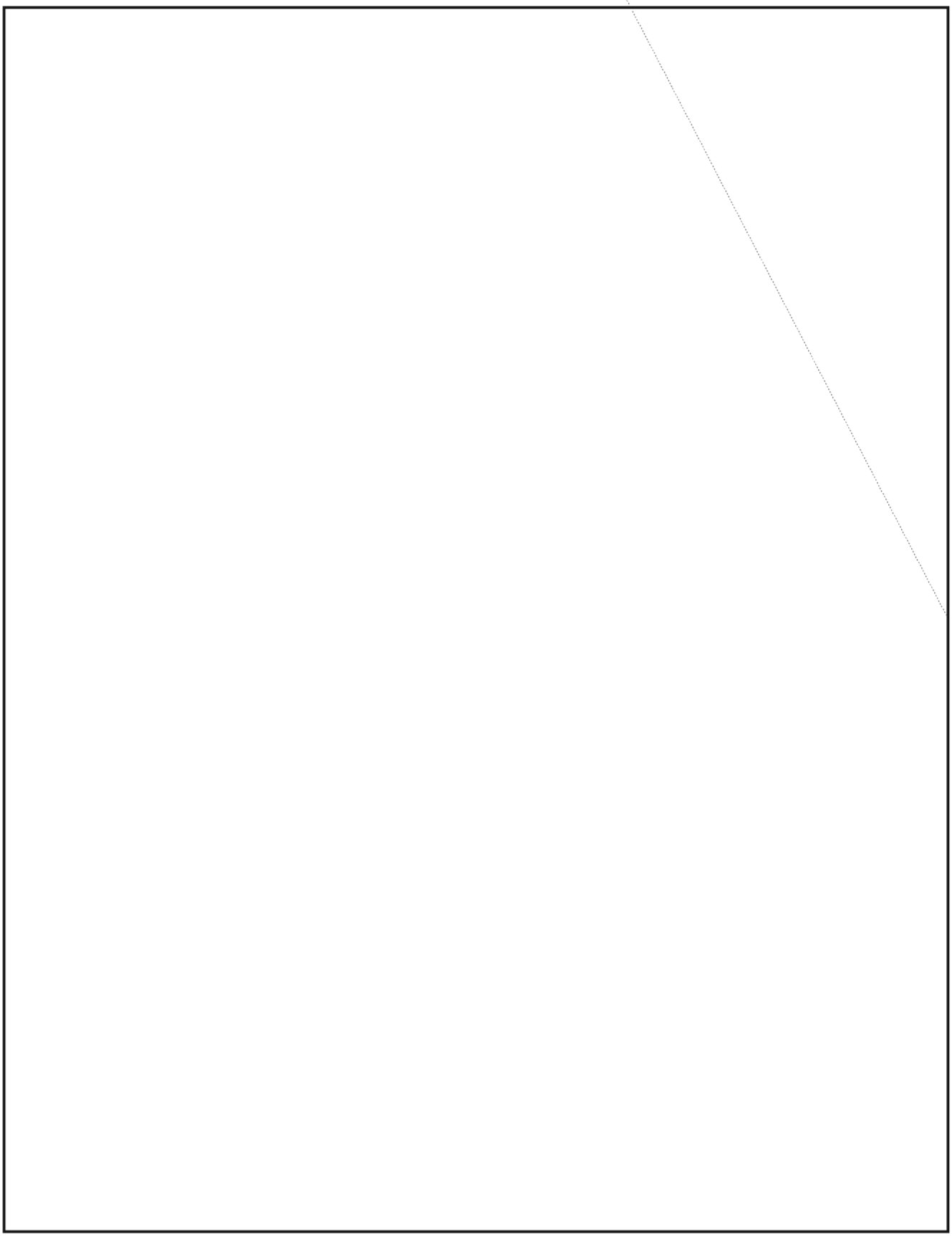
H: That would be great! How can we get in touch with you?

R: We are located in 8A134 and our phone number is 963-1171.

Thanks for giving me this chance to explain what we do, and remember, we're N34 and we're here to help.

[*Exeunt tutti for ice cream.*]

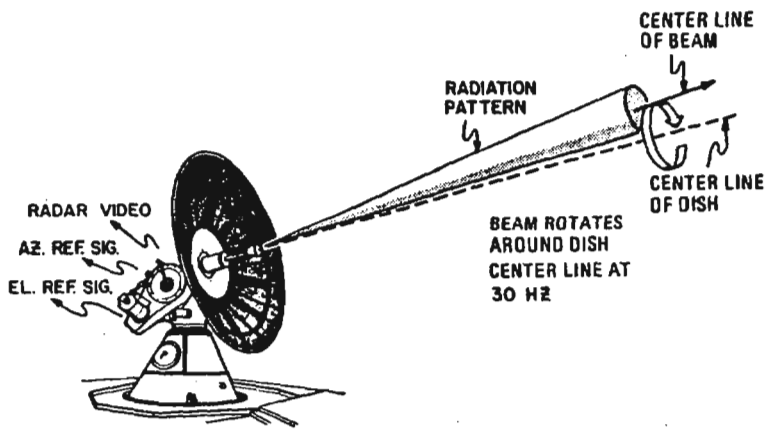
A PROBLEM IN RETRIEVAL (U)



~~CONFIDENTIAL~~

IMPROVING TRAINING IN TECHNICAL ELINT

E54 P.L. 86-36



~~(C)~~ The National ELINT Plan dated 25 March 1985 identifies nine training and retention issues in Section VII, 3. Of the nine issues, four are considered to be actual training issues and they cover such things as:

(1) standardizing ELINT training throughout the community;

(2) designing a series of mandatory continuing self-study courses to expand the knowledge of ELINT people in the field;

(3) modernizing courses to reflect advancing technology;

(4) familiarizing non-ELINT people with ELINT operations.

As a result of this plan, the National Cryptologic School (NCS) has scheduled SIGINT Training and Advisory Committee (STAC) meetings for the 2nd QTR FY86. The STAC meetings will be convened to gather all interested parties together to obtain a corporate review of ELINT training. They will:

(1) Assess the impact of HQ, NSA/CSS and Service operational requirements on training;

(2) Review the impact on training of projected changes in operational targets and technological advancements;

(3) Identify the job performance requirements and training necessary to improve operational effectiveness;

(4) Assess the adequacy of existing training;

(5) Recommend to the Assistant Director for Training changes to training that will improve operational effectiveness and keep pace with projected needs.

A solution to the familiarization problem has already been accomplished by the new exportable IS-070 course which is available, worldwide, as a prerequisite to IS-250 (SIGINT Reporting). It is also teaches non-ELINTers about OPELINT and the differences between OPELINT and TECHELINT.

~~(C)~~ Basic technical ELINT training has traditionally been given at three service schools: Naval Technical Training Center (NTTC), Corry Station, Florida; Keesler AFB, Biloxi, Mississippi, and Ft. Devens, Massachusetts. On November 6, 1985, the United States Air Force transferred its basic ELINT training course to Goodfellow AFB, Texas. All intermediate and advanced level training has been conducted at NCS. These are the technical ELINT courses now being offered:

ARMY	233-98J	Electronic Warfare/Signal Intelligence Non-Communications Collector 402 Hours (Basic Course)
	233-98J30	Electronic Warfare/SIGINT Non-Communications Interceptor 290 Hours (For assumption of duty at E6 level)
NAVY	A-231-0028	Cryptologic Technician--T Field Operations Type FOUR (ELINT Operations) 480 Hours (Basic Course)

~~CONFIDENTIAL~~

TECHNICAL and OPERATIONAL ELINT

Technical ELINT has the signal as its primary focus.

Operational ELINT takes the radar activity and relates it to a radar site, a weapon, a platform or an event.

Examples of the differences are shown below:

TECHNICAL	OPERATIONAL
Signal Descriptions	Emitter Deployment
Emission Characteristics	System Employment
Modes of Operation	Activity Levels/Schedules
Emitter Functions	Weapons System Tactics
Weapon and System Associations, Capabilities, Vulnerabilities	Platform Recognition
	Force Composition
Foreign Technology Indications	Indications and Warning

USAF	E3ABR20530	Electronic Intelligence Operations Specialist 628 Hours (Basic Course)
NCS	EA-202	ELINT Measurement and Analysis Techniques 140 Hours (Intermediate Level Civilian, Self-Paced)
	EA-280	Intermediate ELINT Collection and Analysis 280 Hours (Intermediate Level Military)
	EA-380	Advanced ELINT Collection/Analysis 320 Hours (Mixed military/civilian)
	EA-210*	Digital Analysis of ELINT Signals 160 Hours (Mixed military/civilian)
	EA-281*	ELINT Digital Analysis Training 80 Hours (Mixed military/civilan)

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

* *Developed by a contractor.*

REMINDER

CRYPTOLOG is a classified publication. It may not be read in the cafeteria or in other insecure areas.

BULLETIN BOARD

~~(FOUO)~~ Have you written a program applicable to manual cryptosystems? If so, MADCAPS invites you to submit a summary of information about it for inclusion in a compendium it is compiling. Just reproduce the form below, fill it out, and send it to [redacted]Z. (It is necessarily reduced in CRYPTOLOG; if you can't squeeze everything in, ask for a full-size form.) Don't forget to classify! If you have a question, you may call her on 963-1211.

P.L. 86-36

~~(FOUO)~~ At present a draft compendium is available that contains programs submitted up to 15 January. You can obtain a copy from Alice.

****

Manual Systems Survey

Name of process:_____ Category:_____

Function:_____

Type of Data:_____

Type of System:_____

Programming language:_____Computer:_____Operating System:_____

Point of Contact: Name_____Organization_____Phone_____

Brief Description:( )_____

_____

_____

Availability:_____

Comment: ( )_____

_____

_____

****

~~FOR OFFICIAL USE ONLY~~

P.L. 86-36

Letters

To the Editor:

NSA is approaching a milestone of sad significance. As of 1 January 1987, for the first time in its history, NSA will not have a current centralized collection of [redacted] It is an event that should not go unnoticed, for it dramatically reflects the shifting priorities in a bureaucracy that has lost sight of the requirements of intelligence analysis.

NSA will stand alone in the US intelligence community as the only agency with no centralized collection [redacted] This will not be seen as evidence of cost-effective, intelligent management, nor will it inspire confidence that NSA reporting [redacted] is informed and accurate.

If and when this giant step backwards comes to pass, the consequences will be real, and they will be serious in terms of squandered dollars and lost access to invaluable information.

[redacted]
P.L. 86-36

Editor's note: As we go to press we learn that the subscription will be renewed for 1987.

To the Editor:

Re Vera Filby's entertaining limericks in the Sep-Oct 1985 CRYPTOLOG: The limerick about the linguist named Rease reminded me of his cousin, a gent I wrote about in 1969. Here is a copy:

A gloomy defeatist named Reese
Decided to study Chinese,
When asked to select
A fit dialect,
His choice, was of course, Can'tonese.

The editorial staff of the old CLA Bulletin ran a monthly contest from mid-1968 through mid-1969 for language-related lickericks. The prize each month was mighty check for $1.00, and I cleared a cool $4.00 in that year with these ditties. Here are the other three:

There was a pig farmer named Patten,
Who became an M.D. in Manhattan.
Though his patients adored him,
The druggists abhored him,
For he wrote his Rx in Pig-latin.

A great polyglot, Heinrick I. Berman,
Claims his best tongue is hard to determine.
He speaks Polish with polish,
While his French is quite Gaulish;
And, when drunk, he speaks perfect High German.

There was a fine lass, Polynesian,
Whose feature were Classical Grecian
But her giggling betrayed her,
Foolish sounding it made her.
Alas, she spoke mainly Teeheesian.

You might also get a chuckle from this prophetic poem of mine which was published in the Agency's *Quarterly Review for Linguists* in 1970 during the height of Mao's power:

In China everyone will take a vow
That the key to every trouble is,
A panacea double is,
The little red Works of Mao.

This volume is a real wow,
It makes the weak strong again,
The short becomes long again,
The little red Works of Mao.

In Peiching they all know how
The sick will feel fine from
Just reading one line from
The little red Works of Mao.

They tell you with a curt kowtow
That his great work is liable
To outsell the Bible,
The little red Works of Mao.

The farmer behind his plow
Swears the meanest loaf of rye
Is changed to pheasant by
The little red Works of Mao.

Since the volume first took its bow,
China's youth has been bolting from,
They've become quite revolting from,
The little red Works of Mao.

I"ll make a prediction now
Today we're at the peak of it,
Posterity will speak of it
As the little-read Works of Mao.

[redacted]
P.L. 86-36

CRYPTARITHM

by [redacted] P12/G42

Given:

```
  K R Y P T O S
+S O C I E T Y
  C P K I I K C
```

Solve for:

0 1 2 3 4 5 6 7 8 9

_ _ _ _ _ _ _ _ _ _

Every letter represents a distinct digit. When the letters are associated with digits so that the arithmetic is correct, they will spell out a phrase describing the successful cryptanalyst.

SOLUTION TO NSA-CROSTIC No. 60

From "Q.E.D. - 2 Hours, 41 Minutes," by Lambros D. Callimahos. *NSA Technical Journal*, Fall 1973.

"Spencer Akin: Letter to Birkhan.

"Your letter indicates that the purpose of your entering into communication with this office on the subject of the Kryha cipher machine is to make known its merits for consideration for use in the military service. This device has already been well studied and, I regret to advise, was found unsuitable for adoption in the military service."

ANSWERS TO

ETYMOLOGIST'S DELIGHT

(Sep-Oct 1985)

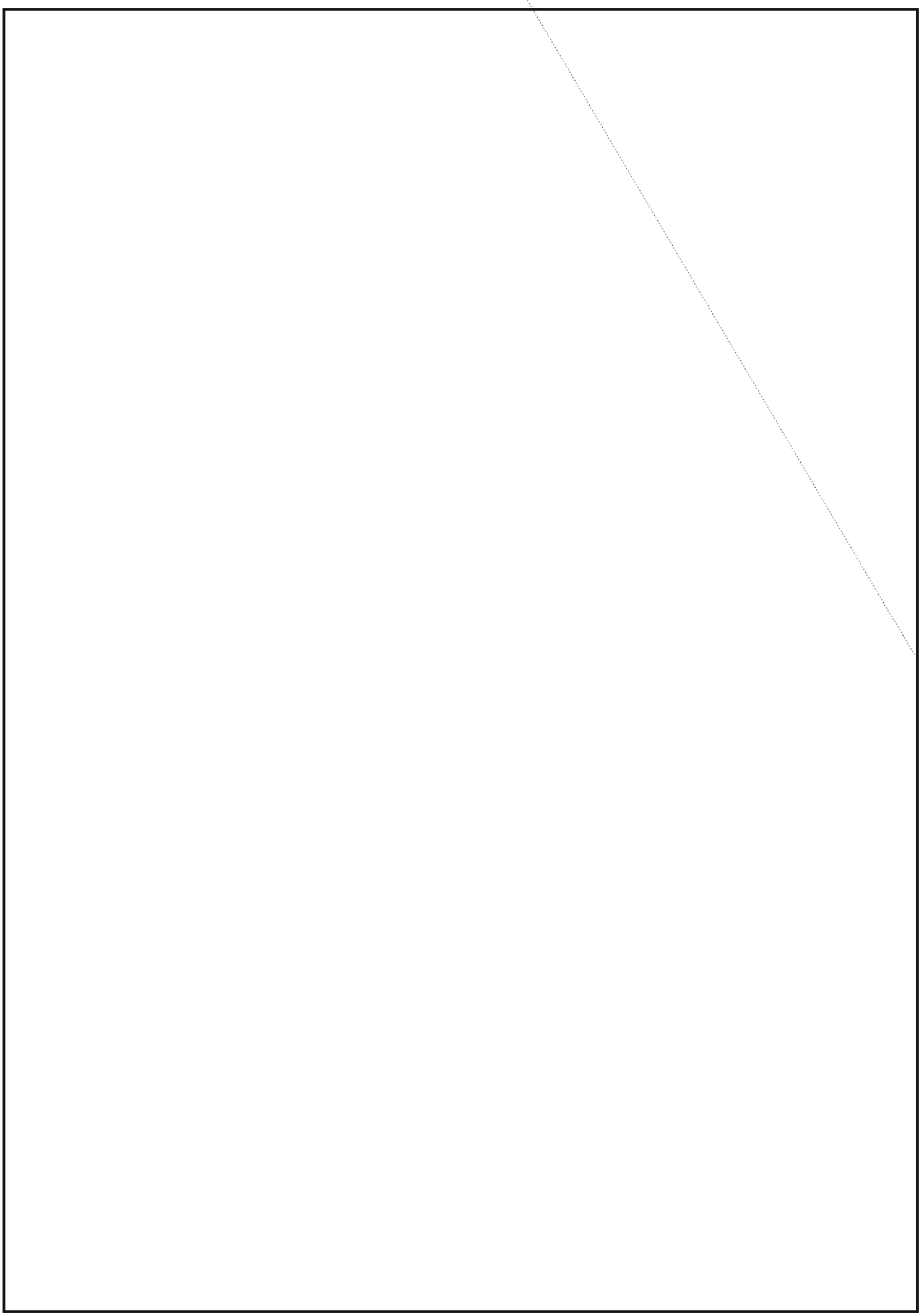
SOURCE LANGUAGES	BORROWED WORDS
Bantu [Sotho]	milo (a sorghum)
Hindi	shampoo, bund (a quay)
Arabic	massage, saffron, soda, mortise, lemon
Tamil [Telugu]	go down
Sanskrit	yoke, Juggernaut, jute, sugar
Malay	catty (a unit of weight)
Algonquin	terrapin, skunk, moose, squash, raccoon
Japanese	tycoon
Turkic	khan
Tibetan	yak, zebu
Turkish	drub, casaba
Breton	menhir
Basque	jai-a-lai
Russian	sable, pogrom
Czech	pistol, howitzer
Narragansett	quahog (a clam)
Spanish	machete, ranch
Norwegian	vole, skull, tangle (seaweed)
Greek	cactus, licorice, skink
Polish	doodle
Celt	barnacle
Gypsy (Romany)	pal
Swedish	addle, mink
French	faucet
Persian	azure, scimitar, caravan
German	snorkel, dowel
Dutch	snook, selvage
Maori	kiwi
Finnish	sauna

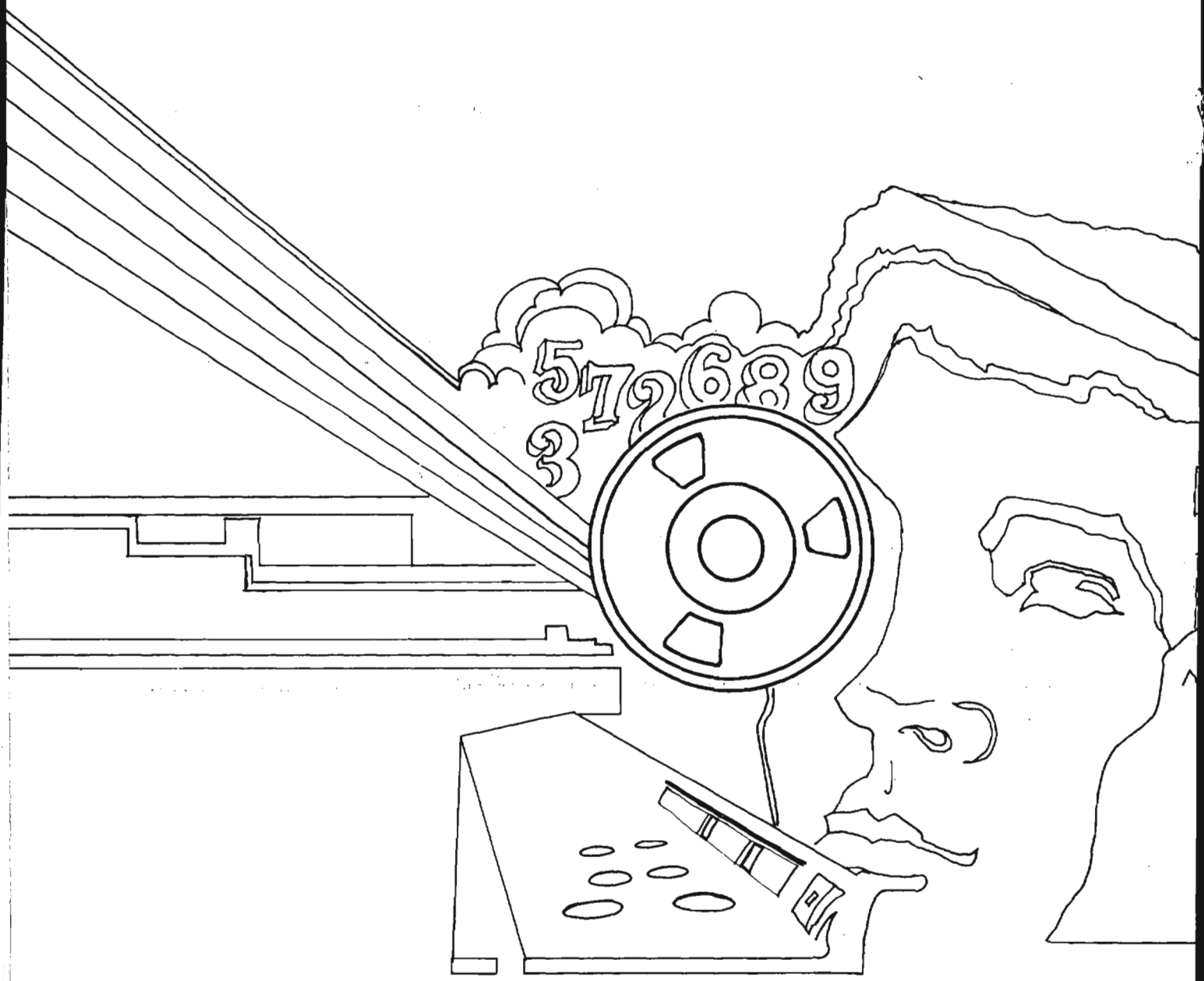
SOLUTION TO

PUZZLE IN PURPLE ⇒⇒⇒

(Nov-Dec 1985)

Provided by [redacted] *P12/G42*




5 7 2 6 8 9
3