Declassified and Approved for Release by NSA on 10-17-2012 pursuant to E.O. 13526, MDR Case # 54778

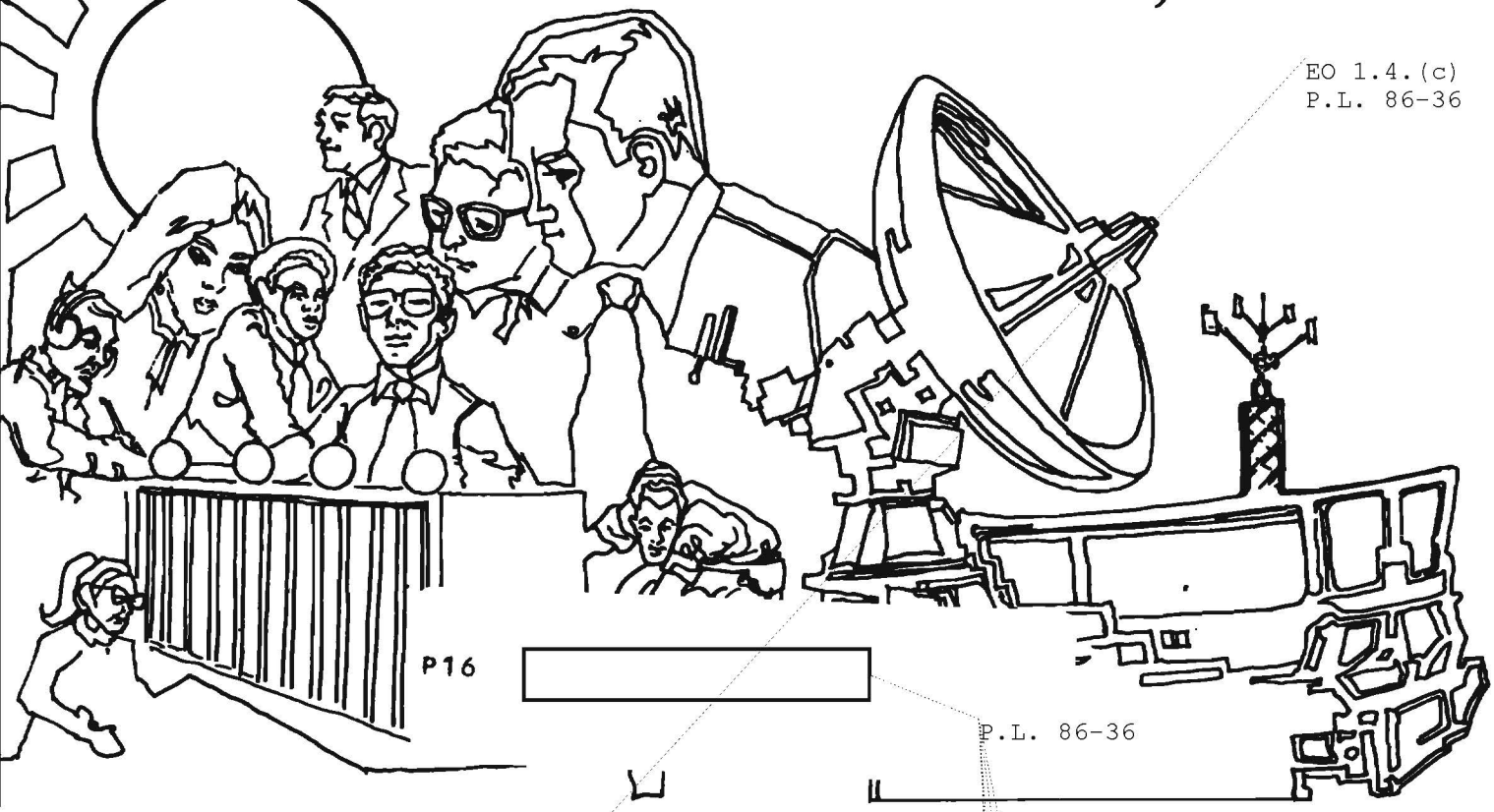
DOCID: 4010912

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

1st Issue, 1987



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

P16

P.L. 86-36

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~NOT RELEASABLE TO CONTRACTORS~~

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

~~SECRET~~

DOCID: 4010012

P.L. 86-36

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XIV, No. 1 ..... 1st Issue 1987

PUBLISHER [redacted]

BOARD OF EDITORS

Editor [redacted] (963-1103)

Collection [redacted] (963-5877)
Computer Systems [redacted] (963-1103)
Cryptanalysis [redacted] (963-5238)
Cryptolinguistics [redacted] (963-1596)
Index [redacted] (963-5292)
Information Science [redacted] (963-3456)
Information Security ..... George F. Jelen (859-1211b)
Intelligence Research [redacted] (963-3845)
Language [redacted] (963-3057)
Mathematics [redacted] (963-5566)
Puzzles [redacted] (963-6430)
Science and Technology [redacted] (968-8075)
Special Research ..... Vera R. Filby (968-8014)
Traffic Analysis ..... Robert J. Hanyok (963-5734)

Illustrators [redacted] (963-3057)
[redacted] (963-6211)

To submit articles or letters by mail, send to:
Editor, CRYPTOLOG, P1, HQ 8A187

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:
NOTE CHANGE: **cryptlg** at bar1c05
(bar-one-c-zero-five)
(note: no 'o')

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

For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, HQ 8A187
Please do not phone.

Contents of CRYPTOLOG should not be reproduced or disseminated outside the National Security Agency without the permission of the Publisher. Inquiries regarding reproduction and dissemination should be directed to the Editor.

A VALENTINE

to

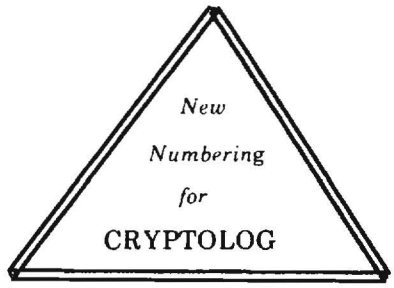
THE FRIENDS OF CRYPTOLOG

Many people behind the scenes make it possible to publish CRYPTOLOG. They are in the Press and in Distribution; they are on the Printing Control Staff; they do data conversion; they review for classification. These people carry out their assigned duties with extra-special TLC. To each of them we send a valentine.

We are also most indebted to our good neighbors in N, the editorial staff of the *Cryptologic Quarterly*, and the system administrators in P044 and in T09 for their bountiful professional courtesy. They very kindly allow us to use their printers while ours is in storage, and rescue us during our frequent crashes. To each of them we send a valentine.

And we are grateful to our colleagues in P1. They are the invisible home team who do odd jobs as needed. To each of them we send a valentine.

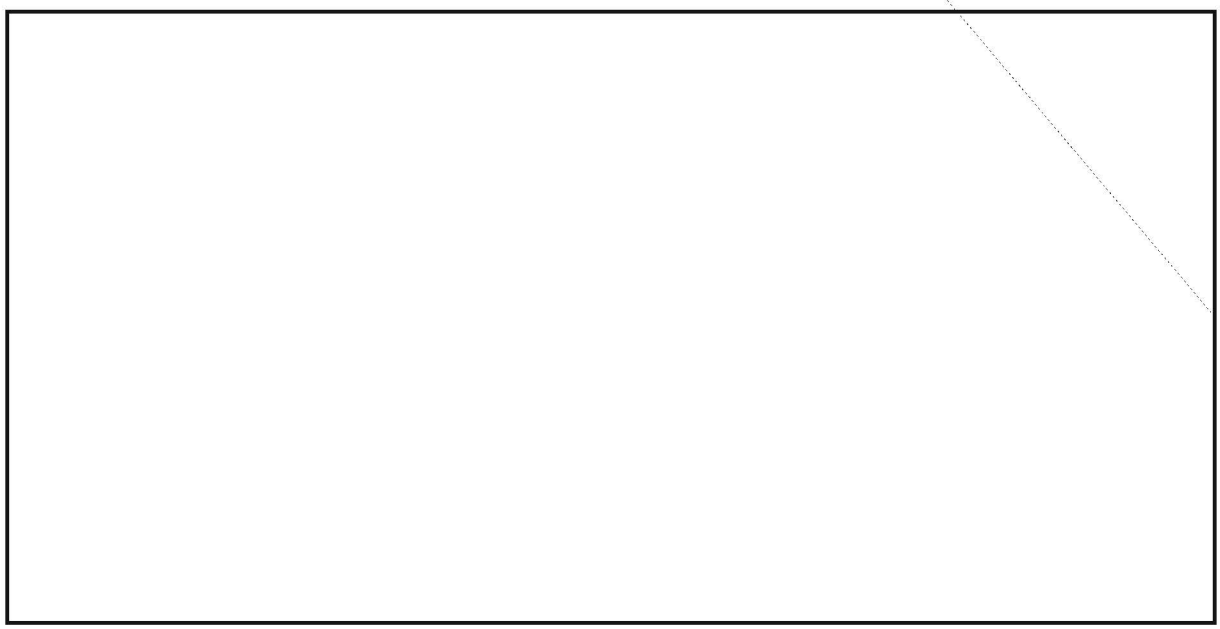
And last but not least, we cherish the many friends among the readers who steer us to the hot items of the day. To each of them we send a valentine.



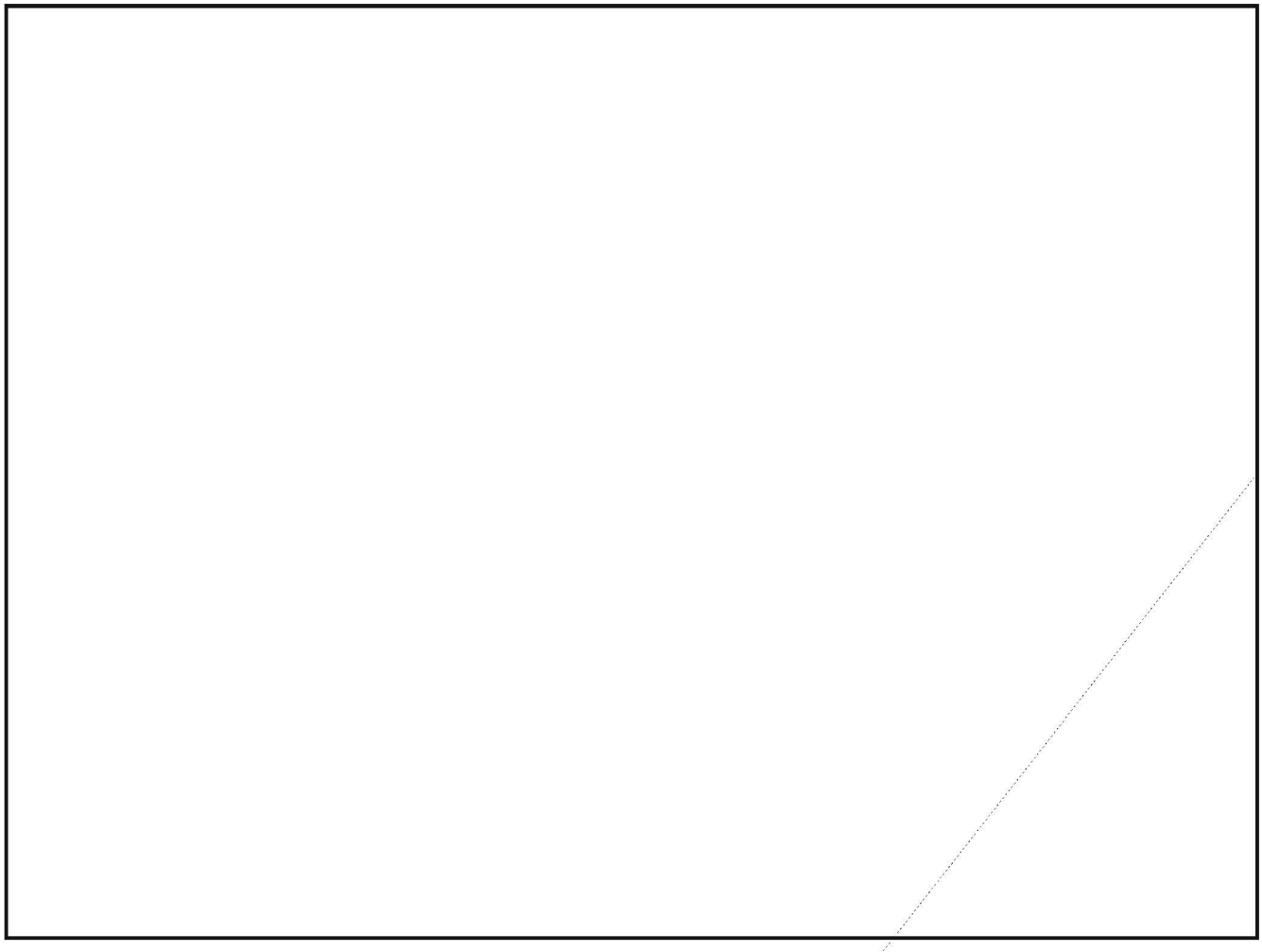
~~FOR OFFICIAL USE ONLY~~

~~SECRET~~

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



P.L. 86-36



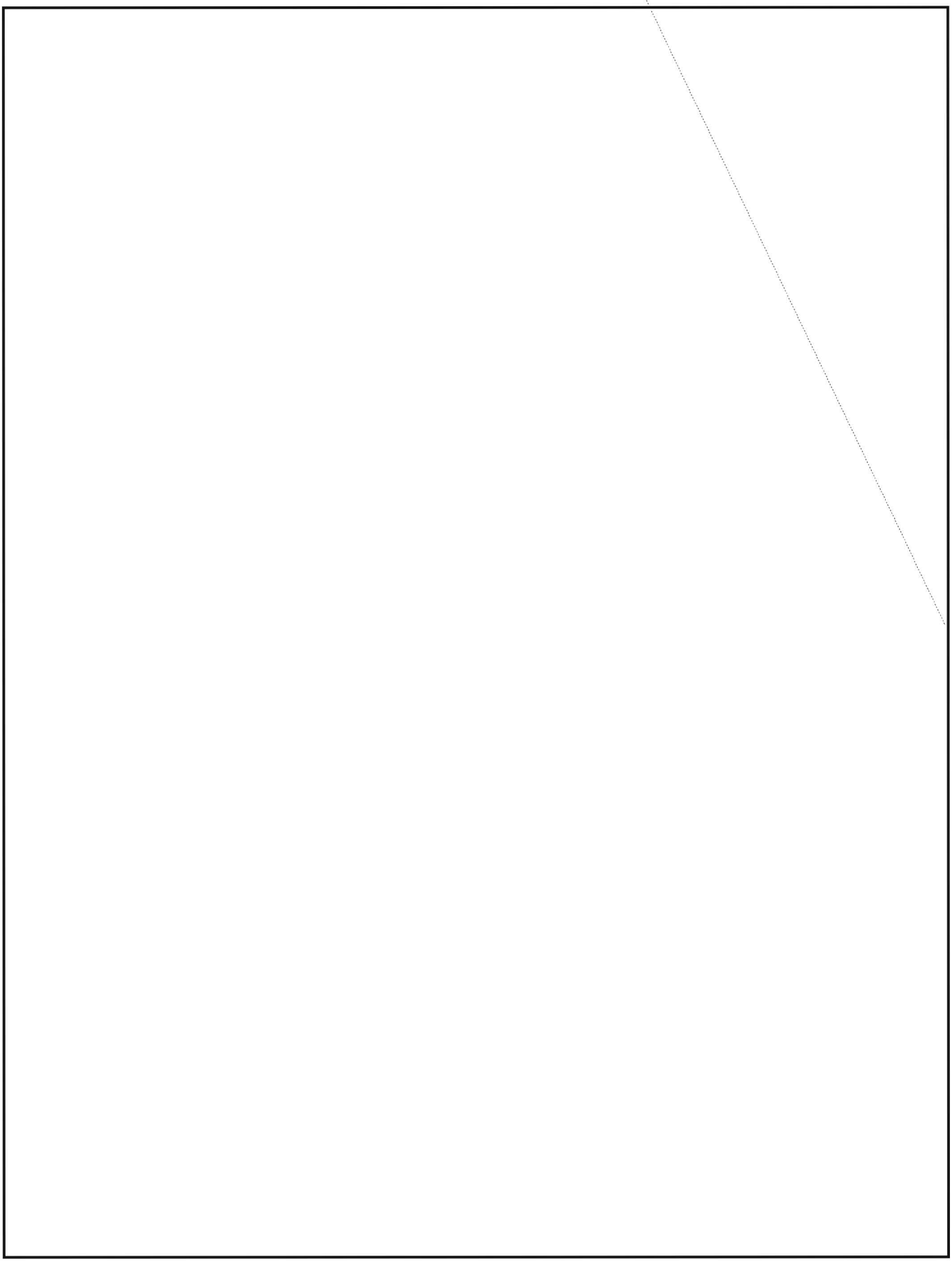
EO 1.4.(c)
P.L. 86-36

~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

DOCID: 4010012

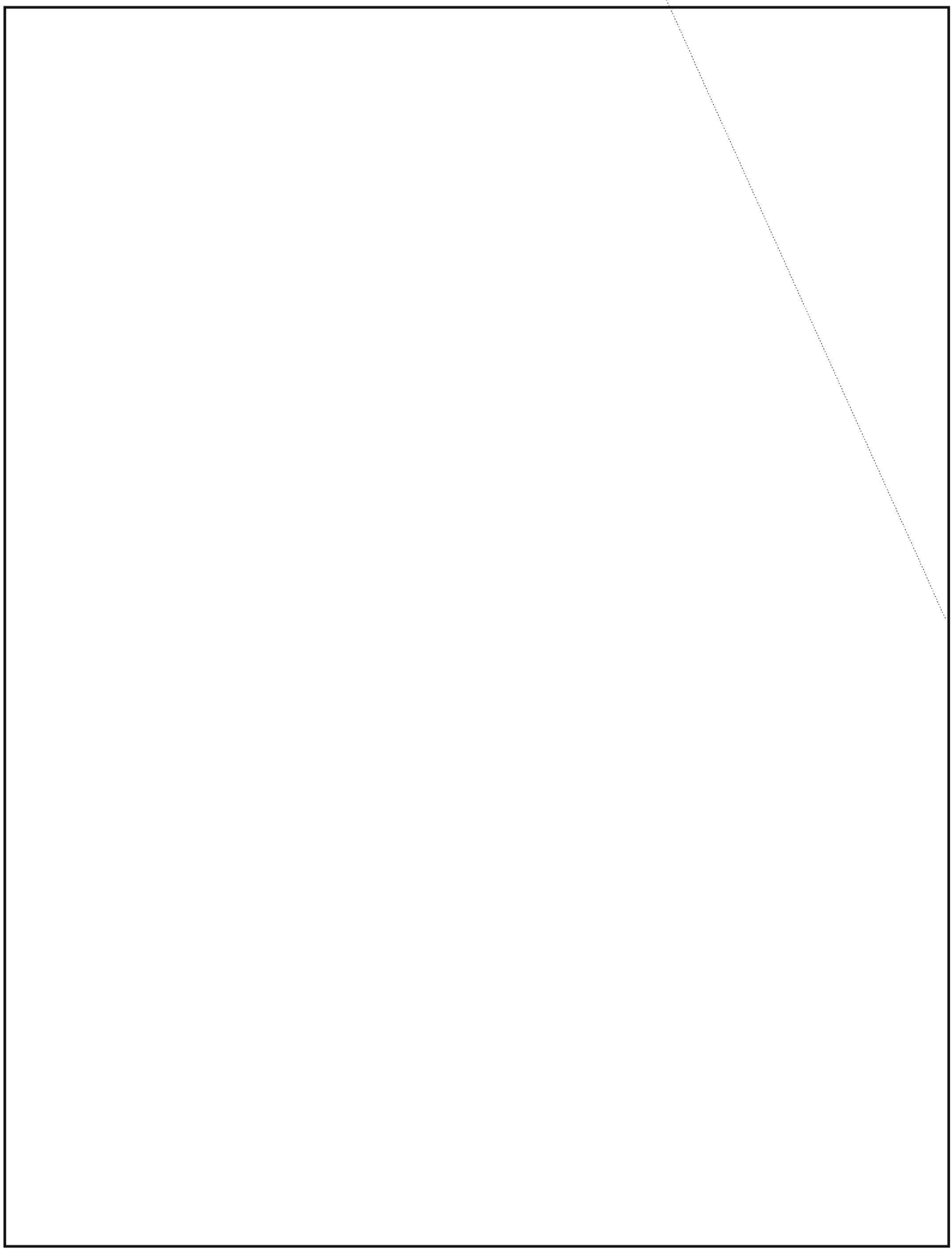
EO 1.4.(c)
P.L. 86-36

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



~~SECRET~~

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

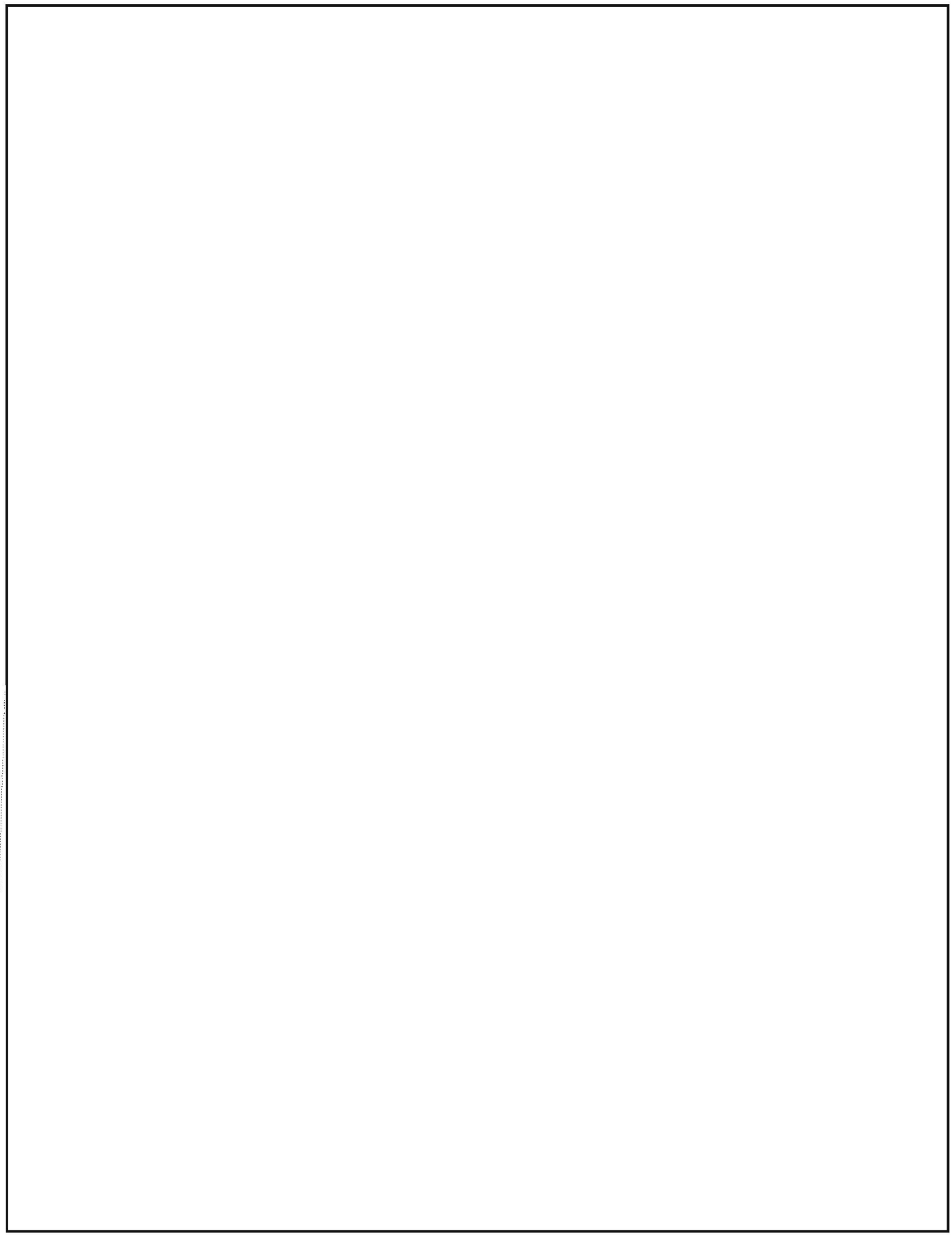


~~SECRET~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

P.L. 86-36



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

DOCID: 4010012

R.L. 86-36

UNITED STATES GOVERNMENT

memorandum

DATE: March 1987

SERIAL:

REPLY TO ATTN OF: [redacted] DSC

SUBJECT: HOW TO WRITE A MEMO

TO: All Memo Writers

1. The purpose of this memo is to provide a set of simple guidelines for writing a memo. My goal is to improve office communications by making memos easier to write and easier to read.

2. The reason for doing this is that I find memo writing in this Agency to be in a deplorable state. Memo structure has long been a particular problem. Trying to find out why the writer sent me a memo and what I am expected to do about it is like solving a whodunit! Grammar is another, but poor grammar is so widespread that I try to overlook it. Lately memos have become rude. "Request." They seem to command me, where a clearer "I request" or a polite "please" would have warmed me to the task of reading the memo and trying to do what the reader wanted. Somehow I have managed to get along with all these problems. But the situation has reached a crisis. Now I find that many memos do not even communicate. I no longer understand what they are trying to say. The time has come to do something about it. Hence this article!

3. My guidelines are:

Present your information in the prescribed order.
Write for the person who is going to read it.
Be brief. Use attachments for details.
Use words correctly and write simply and clearly.
Be polite and courteous.
Be grammatical.

4. A more detailed discussion of these Guidelines is attached.

5. The action to take is this: please follow these guidelines from now on whenever you write a memo.

~~FOR OFFICIAL USE ONLY~~

ATTACHMENT

A memo is, among other things, usually a brief communication that contains directive, advisory or informative matter. So says Mr. Webster! And he is certainly correct so far as NSA is concerned: we use memos in this Agency mainly to advise, inform and direct.

Guideline 1: Present your information in the prescribed order.

Memo structure is designed to assist this process of telling the reader something in the most succinct way possible. Hence, every paragraph in a memo serves a purpose. Look back at the memo in the beginning of this article and notice that I have underlined certain beginning words in three of the numbered sections. These words provide a formula for structuring the contents of a memo. You can't go far wrong if you stick pretty closely to this simple format.

The opening paragraph of every memo should clearly tell the reader why you have sent the memo and what action, if any, you want taken. The advice that Ben Franklin gave to newspaper reporters applies here: this is the who, what, when paragraph. Always, without exception, put this information in the first paragraph. This quickly places the rest of the memo into context for the reader; one reads on with an understanding of what it is one is reading, why one is reading it and what action one must take. Do not bury what you want done in the text where the reader has to hunt for it, or depend on the summary in the last paragraph to do the job.

The next one or two paragraphs convey pertinent information to the reader. Depending on the kind of memo, they may be brief background or history; concise explanatory detail to define or describe the subject (as a reminder or because it's complex); the reasons why you have done something (like "The reason for doing this is" paragraph in my opening memo); the authorities under which you are asking that something be done; or the specific information for which the memo is being sent (such as the "Guidelines" in paragraph three of my memo above).

The final paragraph summarizes the action you expect the reader to take and gives instructions for complying, including the expected due date, a point of contact for questions and a telephone number. If you ever wonder why people don't respond to your memos as requested, perhaps it's because you have hidden this information rather than highlighted it.

Guideline 2: Write for the person who is going to read it.

I'm tired of getting memos that read as if they were written by a computer--stilted, wooden, convoluted and often comprehensible only to another machine! It is easy to write a memo if you write as if you are talking directly to

DOCID: 4010012

someone. The technique works even when you are writing a memo destined for numerous readers. Here are some examples to show what I mean.

A. Dick,

1. This has happened and I'd like you to do so and so about it, please. This one has a short fuse so I'd appreciate hearing from you by ...

2. Here's how it all came about....

3. Please get back to me on this by ... Call my Exec on .... if you have any questions. Thanks very much for your help.

B. Mary,

1. You asked me this question ... (repeat the question) ... and here is your answer ....

2. I got the information by talking to so and so and by phoning some contacts I have at such and such. Everyone (or whoever) agrees with the answer I have given you.

3. If you have any questions about this, or want me to pursue it further, please just call me on ...

C. Jim,

1. We've recently established a new procedure (or committee or organization) and I want to tell you about it. You don't have to do anything, just read on.

2. The reason we have done this is that we saw a need for a new approach to such and such....

3. The officer in charge of this is ..... on extension .... She will be glad to answer any questions you may have. I hope that this new procedure (or committee or organization) will operate to our mutual benefit and satisfaction.

D. Anne,

1. We've recently finished our draft of the PPP Report for the Director and we are now requesting your help in reviewing it. If you

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

can return your comments to us by ...., we'll be able to meet our deadline of .... for submitting the report to the Director.

2. You'll remember that this project, which is designed to ....., started in .....

3. Thanks for your quick attention to this request. My Action Officer, ..., will be glad to answer any questions you may have on ..... Please send your comments to him by .....

Guideline 3: Be brief. Use attachments for details.

If you follow the structure prescribed above, and say what you have to say succinctly, then your memos will be brief and they will also do what you intend them to do--communicate. One of the reasons memos have become so difficult to understand, in addition to being so disorganized, is that they are often far too long and rambling. The reader gets lost in all the unnecessary details if he or she doesn't get bored first and give up reading altogether. Details do have an important place in memos, but that place is in the Attachments. Use the memo text to direct the reader to what is included in the Attachments. Elaborating text, charts, displays, copies of pertinent laws, referenced documents -- these all belong in the Attachments, clearly tabbed and indexed for ease in referring to them. In the memo itself, stick to what you really want to tell the reader, without any distracting information.

Guideline 4: Use words correctly and write simply and clearly.

Memo writers often succumb to the temptation of trying to impress the reader. The irony is often that the writer displays ignorance instead by using words incorrectly. "Enormity" is a good example. It sounds so important and impressive. A thing can hardly be bigger! But "enormity" doesn't mean hugeness, it means wickedness, outrage or crime. When you exclaim that "The enormity of this project overwhelms me" you are saying, "This project is so crooked that I can't stand it." "Viable" is another good example. Does anyone really know anymore what it means? Popular usage is eroding nice distinctions and making communication more difficult in the process.

Even if you use a fancy word properly, it is not necessarily in good memo writing taste or style to use it. Aim for elegant simplicity which is always more desirable in a memo--and usually safer. Don't ever write anything that will send your reader to the dictionary! Always remember that you are trying to tell your reader something important and you want to make sure it is understood quickly and perfectly. Brief memos help you to write clearly and simply. They don't leave much room for lengthy words or text.

I also recommend an informal style for most memos, as you can see from my examples above. Don't be afraid to use informality when it is suitable. An informal style makes it easier to write simply and directly and to avoid the

~~FOR OFFICIAL USE ONLY~~

stuffiness many memos have, or the appearance that they were written by a computer.

Guideline 5: Be polite and courteous.

Whatever has happened to the little word "please"? Nowadays memos all seem to issue commands, the most popular of which is: "Request." That's all, just the bald command: "Request." I realize this was once an acceptable usage but it is no longer desirable. It is jarring to the modern ear. At the very least you should say "I request so and so" (or "urge," "suggest," "ask," etc.). But even better is "Please do such and such," or "I would appreciate it if you would do such and so." After all, you are asking the reader to do something for YOU, a favor. You should show that you realize this and are grateful. Ordering a person around is not the best way to get something done for you. A little courtesy goes a long way.

Guideline 6: Be grammatical.

Poor grammar and word usage often interfere seriously with the reader's ability to understand memos. Good grammar is a primary asset in communication and should always be striven for. More on grammar another time.

Author's Postcript:

If you think it's a chore to write memos, I think it's a chore to read most of them. Memos these days tend to start in media res. *They lead off with what should be the middle paragraphs, omitting entirely any introduction to the subject to explain why the memo was sent to me and what I am expected to do as a result. For years I have been reading the last paragraphs of memos first, in order to find out. If you don't believe me, test it out right now on the memos in your box! Reading a memo in the order written is like reading a mystery story in which the whole thing doesn't come clear until the very end. That is good strategy for mystery story writers, but not for memo writers.*

While you're at it, you might count how many memos there are in your box. Busy executives around here all have mailboxes stuffed with memos and only limited time to read them. On a typical day the Chief of Staff plows through some eight to ten inches of them! The Deputy Directors have equally stunning loads. And all other managers and supervisors get their share. Keep in mind that you are writing a memo to communicate something you think is important for the receiver to read and that your reader is probably a very busy person. In such circumstances, you've got to do everything you can to make sure you get your message across, for your reader's sake and for your own.

Editor's Note:

An example of how not to write a memo can be found on page 20. Yes, it's for real! The indicative information was removed.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

□ CHECKLIST
□ FOR
□ NON-PROFESSIONAL
□ INTERPRETERS
□ (U)

by

Harry Obst, Director, Director, Office of Language Services,

and

Stephanie van Reigersberg, Chief, Interpreting Division

DEPARTMENT of STATE

Editor's Note: This article may not be reprinted in another publication without the express permission of Mr. Obst.

This list was prepared by the Office of Language Services to provide some guidance to Foreign Service Officers and others who may be called upon to interpret for high-ranking officials when no professional interpreters are available.

I. Pre-meeting Preparations

1. Do not agree to interpret at a meeting about which you have not been briefed in advance or if the subject matter is totally unfamiliar to you. Make sure *in which direction* you are supposed to interpret. You may be able to handle Russian into English but not English into Russian. Make sure that you are not expected to do *simultaneous interpreting* (involving equipment and usually teams of two or more interpreters) unless you have had training and experience in it. This is best left to professionals, and even some of them can handle only consecutive interpreting.

2. Make yourself aware of the circumstances surrounding the meeting. Read up on the issues to be dealt with. Ask for the minutes of prior meetings if available.

3. Read briefing materials and talking points carefully with a view to saying their contents in the other language. Be sure you know what all the acronyms mean and how to say them in both languages.

4. Do not underestimate the difficulty of rendering some simple *sounding* English phrases and expressions in other languages. (Try to say "I am looking forward to working with you" or "we hope to be forthcoming" in the language into which you will be interpreting, for example.) Likewise, *do* work on rendering the exact psychological/emotional "charge" of expressions in context, not just the dictionary equivalent.

5. Try to obtain and read the biodata on the participants before the meeting.

6. Speak to the person arranging the physical set-up for the meeting and arrange to sit in the proper place. In general (there are expections) this means the following:

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

a) next to your principal if you are interpreting for him alone,

b) between the two principals if you are to interpret both ways,

c) to the principal's left if you are at a conference table or if the meeting is a meal.

7. Find out in advance *how many* persons need interpreting assistance. Do not assume it is the principal alone just because you were asked to interpret for him or her.

8. Find a moment to ask the principal directly (or if necessary, ask one of his staff) how he wishes to proceed. If he asks for full consecutive or whispered simultaneous interpretation and you feel that you are not able to perform well in one of those modes, tell him *before* the meeting starts. If you are uncomfortable in both techniques, ask him to go a sentence or so at a time.

9. Make sure you have two pens and a note pad with you at all times. Use a *small* note pad at public ceremonies, formal dinners, etc. A legal size pad is not easily carried in the shuffle (security, reporters, waiters) and it spoils the pictures taken by the media and the official photographers.

II. Conduct During the Meeting

1. The golden rule for the placement of interpreters is simple: "*Sit where you can clearly hear* what needs to be interpreted." Do not be shy about moving if you are shunted off to a spot where the speakers are inaudible. Speak clearly and with self-confidence, loud enough to be heard by everybody, but not louder than necessary.

2. Speak in the first person. Never say, "He says to thank you for coming," or use any form of indirect discourse.

3. Avoid interjecting any personal opinion of the "he says but probably means . . . " variety. As a substantive officer you may worry when your principal strays from his talking points, but as an interpreter your role is to present a mirror image in the other language of what he is saying. In short, do not summarize *or* censor.

4. Do not draw out the interpretation of the social niceties at the opening of the conversation. Move through this at a faster clip, as the principals are already losing much of their allotted time due to the need for interpretation. Conversely, make sure to slow down a little and to apply the necessary emphasis when you interpret an important point or come to the crux of the message, so the principal will not miss it.

5. If the speaker talks too long for your skill level, politely remind him that he should pause for interpretation. Do not be embarrassed about this, because you are there to provide a service, a communications link, not to put on a bravado performance.

6. *Stay close* to the principal during stand-up and walk-around receptions and similar situations. The principal must be able to summon you in *5 seconds*. Do not get involved in you own socializing and let him drift away.

7. Pace yourself. Don't give everything you've got in the first 10 minutes -- you may have to keep at it for an hour or more.

8. If you are called upon to interpret a toast you may write it down (if you don't have the text in advance) where you are seated, provided you can hear clearly. However, at least while you deliver it, stand with your principal and do your utmost to project the same atmospherics as he does (cordiality, friendliness, etc.) Be sure to look up at the guests occasionally.

At the end of the luncheon or dinner speech when you come to the toast itself, it is advisable to depart from the rule that the interpreter always speaks in the first person. If the guests have already drunk the toast, because so many of them understood the speaker and are now seated listening to the interpretation, switch to the third person and past tense at the very end and say, for instance, "and then the Secretary *raised*

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

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

his glass and *drank* a toast to the health of the President and to the continued prosperity of . . . "

III. After the Meeting

1. In most meeting there is a notetaker who will write a memorandum of conversation.

If in the course of an interpreting mission you found yourself briefly alone with the principals, with no notetaker present and something of substance or importance being communicated, go to the principal's chief aide after the meeting and volunteer to write a memorandum of conversation on that exchange. He will instruct you how to write such a memo or may be satisfied with an oral debriefing. This obviously does not apply if your principal instructed you to make no record.

2. Return all classified briefing material and destroy your notes if no memcon is needed. Do not retain any copies of the memorandums of conversation. Destroy or surrender your interpreting notes after the memorandum is finished, unless you are instructed to hold them until after the memcon is reviewed and accepted. □

Golden Oldie

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

Solution to NSA-Crostic #63 (plus)
(December 1986)

[Lambros D.] Callimahos, *Ars Conjectandi:*
[*The Fundamentals of Cryptodiagnosis*]

DEFINITION:

"*diagnostician*, [n.]. An experienced cryptanalyst of ability just before retirement age."

This is but a gentle reminder to the reader of an aphorism of Hippocrates, as translated by Chaucer: "The lyf so short, the craft so long to lerne."

PLUS: *The Bonus (or Clue, as the case may be) is in the fifth position down, and reads:*

FIND HIDDEN MESSAGE. CALL DLP

WHAT'S A NICE CRYPPIE LIKE YOU DOING IN A PLACE LIKE N? (u)

P.L. 86-36

[redacted] *A509*

This article is classified ~~CONFIDENTIAL~~ in its entirety

Quitting time, April, 1985: I was on my way out the door when the secure telephone rang. "Ms. Wilson, GALAXY has surfaced your name as a top candidate for a position in M3."

"M3? Personnel? What does Personnel want with a cryptanalyst?"

"*N*3, not *M*3." (Payroll is going to encrypt paychecks?) Curiosity being inherent in cryptanalysts, I agreed to an interview, and began one of the hardest, fun jobs I've had in 18½ years at NSA.

A certified cryptanalyst, I had never worked outside DDO; worse yet, except for my intern tours, I knew little outside the workings of A5. Oh, there were occasional conversations with G4 and W3. But with regard to the mission of the Agency overall, I was a cloistered nun dedicated to the worship of bits, ignorant of any larger world outside my cell.

And what was this hardest fun job? Very simply, to look at, from an overall Agency point of view, all of the projects in support of cryptanalysis. [redacted] I got to look at the planning and to recommend approval of the money and actions. AWESOME!

P.L. 86-36

Yet my power was not inordinate. I really could only recommend a position to the Deputy Director for Programs and Resources, (DDPR) through a chain of Division Chief, Office Chief, and Group Chief. That kept me humble. I was often grateful that my view as the sole cryppie in DDPR was tempered by the perspectives of the very experienced managers in the N3 chain.

All the while the time clock was ticking away at my tour in DDPR. Two years in N342 was considered optimal, after which I was expected to go back into the DDO mainstream. In the meantime I would be part of a select group in N342, known as System Management Officers or SMOs, each of whom was a resident expert for a different discipline: signals analysis, language analysis and voice processing, telecommunications, collection, computer science, intelligence research, engineering, and of course, cryptanalysis. After two years out of the mainstream, the theory is, SMOs lose touch with what is happening in the trenches in their field, and fresh blood is needed to provide a current perspective. Also, the period of two years allows the SMO to participate in at least two budget cycles and to learn how the

Agency gets money; this is an excellent ticket for managerial positions.

As the resident cryptanalyst in DDPR, nominally my job was twofold: 1) to enforce NSA Circular 25-5; and 2) to advise the DDPR on cryptanalytic programs from a macro, overall NSA perspective.

The DDPR, as the Agency Directorate for Programs and Resources, is responsible for making sure that NSA acquires needed resources and spends money responsibly. And we must account to three layers of oversight: Department of Defense, Director of Central Intelligence and (always) Congress. A primary mechanism for insuring adequate planning and senior review/approval is NSA Circular 25-5 ("That blankety-blank 25-5!"). It calls for documentation of all NSA initiatives (projects) costing $2 million or more, with coordination and review by appropriate Agency-level authorities at specific decision points in the acquisition.

[redacted]

P.L. 86-36

[redacted]

These necessary coordinations allow L to plan space, T to plan comms circuits, E to gear up for new training courses. And as the details are being worked out, it gives you a chance to clarify the points that the engineer misunderstood:

[redacted]

Finally, the engineer writes a plan laying out the details of how to get your processor, assigning responsibility to any OPI that will be involved in getting your "system," and showing a schedule of milestones for keeping the acquisition on time.

This is a System Acquisition Plan, and again, you and appropriate offices in L, T, E, etc. will coordinate and have a last chance to make it say what you want it to do. Once it's coordinated, it is the record documentation for your project or acquisition, and the engineer can now put out Procurement Requests (PRs) to buy whatever is needed.

As DDPR's coordination staff for 25-5 documentation, the N34 SMOs review all of these papers. DDPR is one of the few places where all of NSA's efforts on a specific problem can be viewed for both serious holes and wasteful duplication. The budget resource managers in N2 understand the figures and totals and how to balance the overall NSA budget. They do not, however, have the technical expertise to understand the actual impact of budget cuts on the people in the trenches and on the work itself. The perspectives of the N34 SMOs, who are evaluating the efforts and who can see the real effect of a projected cut from the point of view of the working cryptanalyst, signals analyst, etc. enable the DDPR to operate with better understanding.

The biggest problem I had was my desire to save *every* project that came across my desk, because each one addressed what I considered to be a valid cryptanalytic need. Sometimes I succeeded in rescuing a program from the budget cutters or from shooting itself in the foot because of poorly written justification. While I was sometimes likened to a terrorist for enforcing 25-5 and related controls, just as often I was thanked by the sponsor, the user,

or even the developer, as being the policeman on the beat who came to their rescue when a project was being hijacked in political power plays, or threatened by budget cutters, or abandoned because of resource crunches.

Behind-the-scenes liaison with senior staffs was common, and I really came to understand the organization of NSA for the first time in my career.

Visibility was tremendous, for better or worse. I briefed DIRNSA as well as the Deputy Directors on an aspect of Advanced Modulations, and I briefed the Assistant Director for Installation and Logistics on an anticipated avalanche of future projects . And senior managers in R and T, (places I never even knew existed when I was in A544), bandied my name about.

I also realized that cryptanalysis was in much better shape than I would have guessed from my futile attempts when I was in A544 to get money to upgrade some obsolete collection positions.

A hard job? You bet! The responsibility for reviewing and evaluating cryptanalytic projects across the board is serious and mentally draining. But definitely a fun job! For it means that you get to see from start to finish, everything the Agency is doing in your field, and have a chance to comment on it. What a tremendous opportunity!

And that's why a nice cryppie (or signals analyst or linguist, etc.) should consider going to a place like N. □

BULLETIN BOARD

FOR GERMAN LINGUISTS

(U) Taped German radio programs with transcription, glossary, and extensive cultural notes can be loaned to interested individuals. The program is *Schau ins Land*, produced 14 times during the academic year. Write to [redacted] P16, HQ 8A187.

P.L. 86-36

OLD PHOTOS WANTED (U)

(U) Do you have any old photographs that illustrate an aspect of Agency history? A picture of an intercept site? Photos of obsolete R&D projects? Candid pictures of NSAers at work? Formal ground-breaking or VIP visits?

(U) Whether they are organizational pictures incorporated in an old briefing, or personal photographs stored in your desk, they might of interest to the History Program. NSA now has han official archive of historical pictures, maintained by T54.

(U) If you do have some pictures that illustrate an aspect of our history, and you can identify the subject and date with reasonable accuracy, please let us look at them. If you need the originals back, we will make a copy for the Photo Archives.

(U) We also accept donations of photos and slides, positives and negatives. Call [redacted] or [redacted] 972-2355.

P.L. 86-36

FOR CRYPTOMATHEMATICIANS

~~(FOUO)~~ NSA has a resource which every cryptomathemician should know and use. It is the R51 classified mathematics library, located at FANX-III, Room B2B37, and presided over by librarian [redacted] This collection of papers contains some real gems of mathematical cryptology dating from the years of World War II as well as much significant research of more recent times. It is well worth a trip to discover this reservoir of interesting and useful material. Mrs. [redacted] can be reached on 968-8580s.

CRYPT PROBLEMS WANTED

~~(FOUO)~~ KRYPTOS and the NCS will be publishing a series of problems in cryptanalytic diagnosis that will be representative of current target systems. The intent is to publish the problem in one issue and the annotated solution in the subsequent one. It will be designed so that the set of solutions can be bound, and thus collectively form a diagnostician's desk reference.

~~(FOUO)~~ We request your assistance in finding suitable problems. They should be non-trivial but capable of at least a partial diagnosis on the basis of a small sample and/or a statistical summary. If you have such problems, classified no higher than TSC, please check with your management first, then get in touch with [redacted] P15, 963-3957.

P.L. 86-36

DOCID: 4010012

FROM THE PAST

UNITED STATES GOVERNMENT

memorandum

SERIAL: Xxx/xxx/72

4 May 1972

X. Xxxxxxx/xxxx/xxx

REPLY TO ATTN OF: Xxx

SUBJECT: Xxxxx Xxxxx Contact Reporting Xxxx (Xxxx-xxx)

TO: Xxx, Xxx

REFERENCES:
a. XXXX-3-100, 4 Apr 72
b. X/xxxx/xxxx/x, 27 Mar 72
c. Xxx-066-72, 4 Mar 72
d. Xxx-065-72 4 Mar 72

1. Inclosed for your action is a copy of references a and b (which respond to references c and d). A copy of references d, e and f cited in reference b above has been also inclosed for your convenience. Two copies of reference c (XXXX/XXX-Xx) cited in reference b, were forwarded to Xxxx by XXX on 19 February 1971. The delay in forwarding this material was caused by the necessity to obtain a copy of reference f cited in reference b above from XXXXX.

2. Please forward your comments on reference b above to Xxx so that a response may be prepared and sent to XXXX-X as requested in reference a.

/s/ Xxxxx X. Xxxxx
for Xxx X. Xxxxxxxx

Chief, Xxx

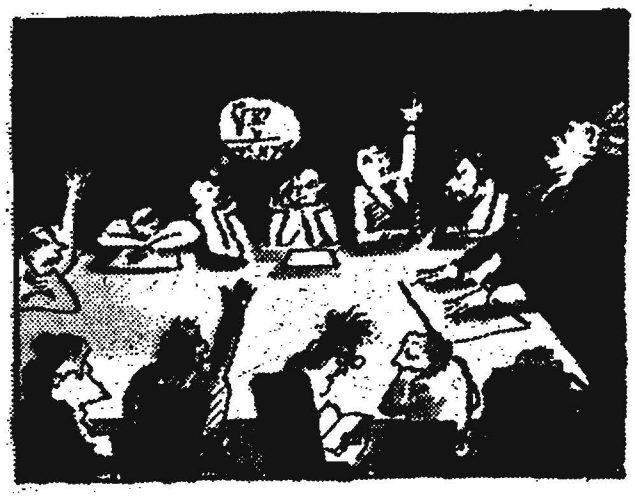
Incls:
a/s

cc: Xxx (less incls)
Xxxx "
Xxx "
Xxx (refs a and b only)

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

Conference Report



The 1987 Joint Mathematics Meetings, San Antonio, Texas, 20-26 January 1987

Reported by: David Harris, R513

This is the national meeting of the two major mathematics societies, the American Mathematical Society (AMS) and the Mathematical Association of America (MAA), along with some other organizations. It drew some 3500 attendees.

NSA personnel in attendance were: [redacted] and the author. Some of us concentrated on talking with colleagues, making contacts, and studying recent developments in mathematics and statistics. Others were engaged in formal recruiting.

Also in attendance were individuals who are associated with NSA or with IDA/CRD: [redacted]

Among the other attendees were notables in mathematics from industry and academia.

The following is a summary of my own view of the major points of interest at the conference. For reasons of space only a few of the mathematical papers are summarized here. Additional information and some of the papers can be obtained from the attendees.

BENEFITS OF ATTENDING

It is important that the Agency continue to be represented at such conferences. It provides us with an opportunity to talk with outside mathematicians and to follow developments, and thus enables us to monitor the mathematics done in the public sector.

Conferences also give us an opportunity to improve public relations. DoD continues to have public relations difficulties with the mathematics community, and this has affected our recent efforts to establish a funding program for outside mathematical work. By attending these conferences we are in a better position to anticipate what the problems will be and to develop strategies for meeting them.

Much of the benefit from going to conferences derives from informal talks with mathematicians, as we had with Thurston, Calderbank, Diaconis, Kailath, Nevai, Askey, and Lax, detailed below. We get to be considered as human beings and so become less threatening to the academics. Through informal talks we learn more readily what we may expect in the way of technical breakthroughs. While we run the risk of giving academics information on our capabilities, we

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

also get to judge how close we are to the outside state-of-the-art.

PERCEPTIONS OF GOVERNMENT FUNDING FOR RESEARCH IN MATHEMATICS

Attitudes have changed for the worse in the last two years. At present, academic mathematicans are generally not very friendly to government or to DoD, though many think that they should get support through the National Science Foundation almost as a matter of right. This was evident at the AMS business meeting during a debate on DoD funding of academic mathematics, SDI, and the proper relationship between DoD and academic mathematics. Opponents of DoD pretty much controlled this meeting, though in fact it was poorly attended and only a few people were involved in the debate.

Agency personnel interested in our recent effort to build bridges to academia should study the debate to learn what does not work and what problems must be overcome.

On the positive side, NSA attained Corporate Membership in AMS at the Council meeting, attended by Alberts, Liebler, and Morris. Selfridge spoke on our behalf during the discussion on our membership, citing the favorable impression he gained at the recent NSA Conference. He also responded to a query about what NSA does, drawing on information he had gleaned at the NSA Conference.

THE AMS BUSINESS MEETING AND THE DEBATE ON DoD FUNDING OF MATHEMATICS

The board voted to call for a major increase in the NSF budget and for the AMS to sponsor mathematics competitions for students.

Under the rules of the AMS, before a motion can be adopted it must be considered at two business meetings. At the first, it is voted onto the Agenda of the second, and at the second it may then be formally adopted. Accordingly, there were four motions at this business meeting relative to the following two resolutions:

Resolution 1: Many scientists consider SDI (commonly referred to as Star Wars) incapable of achieving its stated goals and dangerously destabilizing. Participation by universities and professional organizations lends a spurious scientific legitimacy to it. Therefore the AMS will lend no support to the Star Wars program. In particular, no one acting as a representative of the AMS shall participate in efforts to obtain funding for Star Wars research or to mediate between agencies granting Star Wars research money and those seeking to apply for it.

Resolution 2: The AMS is concerned about the increasing militarization of support for mathematics research. There is a tendency to distribute this support through narrowly focused (mission oriented) programs which circumvent normal peer review procedures. This tendency, unless checked, may skew and ultimately injure mathematics in the United States. Therefore those representing the AMS are requested to direct their efforts towards increasing the fraction of non-military funding for mathematics research, as well as towards increasing total research support.

While the action parts of these resolutions are mild and apparently designed to achieve consensus, the preceding rhetoric is not. The first two motions were to put these resolutions on the Agenda at the Salt Lake City Business Meeting in August so that they may be formally adopted. The last two motions were to put the AMS on record as being in favor of the resolutions.

President Mostow decided to end the meeting on schedule, so he placed severe limitations on time for debate. Ultimately, all of the motions passed by slim margins. Probably none of the motions would have passed had the rules been adhered to. The few vote counts were of debatable accuracy. Attendance at the business meeting was about 200, a tiny fraction of the people registered at the meeting, not to mention of the AMS membership. About 400 AMS members had signed petitions endorsing the resolutions.

Summary of points against the motion:

- There should be multiple modes of funding;
- DoD has the ability to take risks;

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

- NSF funding is increasing as fast as military funding;

- How can anyone object to doing research to see if SDI is valid?

Summary of points for the motion:

- Neither motion inhibits individuals from doing SDI work.

- DARPA money unbalances mathematics towards mission-oriented work and encourages students to enter some fields at the expense of others.

- Priorities should not be set by a military that lacks an overview of mathematics.

- SDI thwarted disarmament at Reykjavik.

- Would SDI be wise even if it was possible?

- The dependence of computer scientists on DARPA is excessive and harmful.

- Suppression of factorizations of integers shows DoD's wickedness.

During the debate in the evening people spoke both for and against the resolutions, but predominantly in support of them.

One speaker focused on proper institutional policies in DoD funding. He supported national security as a valid goal, but he stated that military programs in support of research are highly mission-oriented, secretive, and rely on scientific evaluation procedures of variable reliability. In his opinion, AMS should do nothing to foster substantial funding of mathematical research in this military mode.

What may be more acceptable is defense programs in civilian mode, operated with a reasonable variant of peer review and unclassified, in research areas selected for their general relevance to the funding agency, but with little direction imposed on the individual investigators. He spoke of the dangers of "political abuses" (i. e. non-scientific pressures on investigators or political exploitation of their participation without their consent, as he said has happened in SDI). In the long term he wants a realignment of federal funding so that the preponderance will come from NSF-like Agencies. He believes that recent initiatives in interdisciplinary research should not be allowed to interfere with traditional modalities.

According to him, DoD program managers who understand science have little discretion or influence on scientific policy. He sees that policy makers operate at a level where non-scientific issues are paramount and where the mathematics budget is negligible. He opposes making such a structure responsible for the fate of 40% of federal support for mathematics. He believes that when the nation's interests call for adjustments in the funding of mathematics, the academic mathematicians can talk rationally to NSF. "But whom can we address at DoD who has the power, knowledge, and commitment to basic science to make appropriate changes?"

A second speaker believes that military research does not belong on university campuses, for military organizations are hierarchical and secretive. The size of military grants compared to other sources of funding distorts departments, creating divisive mini-empires, influencing allocation of limited resources, and setting priorities for graduate student manpower. The research initiative approach tends to give givers and takers a common interest in disguising research failures. There is more than enough military research being done already, most of which does not improve military effectiveness.

He cited evidence that money from DoD would be used to quiet mathematicians from criticizing DoD programs. "Military research adds to a threatening atmosphere, particularly between the US and the USSR." Military funding will change mathematical culture, leading it towards classified research and ultimately weapons design. "Mathematics is a poverty-stricken discipline, and we face a shortage of mathematicians soon. This does not mean we should sell out." "If and when a consensus can be reached, the Society should lobby against military funding."

A third speaker gave a reasoned defense of accepting DoD help. He pointed out that others wanted the government's money, and that the government need not beg mathematicians to accept financing. He argued that priorities are set by the *civilians* in Congress and by the President, and that if mathematicians want more money they must show that they are valuable to society on the latter's terms. If

DOCID: 4010012

society values research of practical importance to the national security, then mathematicians ought to consider this. He said he was very disappointed with the business meeting.

A fourth speaker made a passionate statement about the potential damage to the national defense if the resolutions were to pass. Such resolutions may discourage mathematicians from dealing with DoD. Another speaker said reliance on military money is a threat to mathematics. He compared taking DoD money to taking money from the Nazis (He later took this back.) He mentioned the threat to cut off money to people critical of DoD programs. Still another speaker referred to gold-plated toilet seats, cheating, and inequities in grants. He said National Defense is a euphemism for Imperialism. At best, military spending is money down a rat hole.

A New Jersey woman said she had been told by a non-mathematician that she should not teach mathematics because it will help blow up the world. She asked, can we change the perception of the world that mathematicians help the military? With this, someone attempted to recruit more spokesmen for the DoD's side. But since we saw which way the wind was blowing, we felt it pointless to respond and left the meeting.

All this was rather discouraging to those in favor of the new Agency effort to improve relations with academia. The attitude of academics at Louisville two years ago was more in tune with the Agency's present policy of collaborating for the common purpose of improving the health of mathematics in the United States. Those academics at this meeting who made their views known were generally of the opinion that the nation owes them support, that the support should be from NSF, and that money from DoD is more likely to harm academia than help. A substantial minority still view DoD as the enemy of humanity.

It seems clear, however, that DoD ought to give some thought to the effect its grants will have in mathematics departments. Departmental politics may be as important a consideration as national politics in making these grants work. DoD should try to avoid the appearance of trying to set priorities for academic mathematics.

The MAA business meeting was extremely poorly attended. In fact, after the resolution was passed changing a quorum from 25 to 50, a jokester in the audience pointed out that the business meeting no longer had a quorum and so had put itself out of business! Several proposed changes in the bylaws were routinely passed.

INFORMAL CONVERSATIONS

P.L. 86-36

I had informal talks with Askey and Nevai on approximation of the tails of distributions.

Several of us - [redacted] and I - talked to a leader of the faction in favor of the anti-DoD resolutions. I spoke to him about the Agency's new effort to strengthen academic mathematics and attempted to convince him that we are human.

Several times I talked to Persi Diaconis, who was in the Harvard Statistics Dept. in 1972 while I was getting my degree in the Mathematics Dept. I asked him about some of my moments problems. Kailath remembered me from a briefing he gave at Fort Meade.

[redacted] spoke at length to A. R. Calderbank of AT&T Bell Labs. [redacted] supplied Calderbank with several references relevant to his work, and informed him that one of his results had been anticipated in a paper by [redacted] At the urging of Marshall Hall, Calderbank is working on the existence of a design with parameters $(v,k,\lambda) = (28,10,5)$.

Don Rawlings of California Polytechnical State University gave a talk on an extended Simon Newcomb problem. [redacted] took him aside and educated him about a very powerful matrix technique published long ago by Becker and of which Rawlings seemed unaware.

[redacted] talked briefly to Ken Johnson of Penn State, who gave a very interesting talk on quasigroup characters relevant to nonabelian Fourier analysis, Schur rings, and association schemes. In recent papers Johnson and Smith generalize much of character theory to association schemes. Johnson gave [redacted]

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

several of these papers, copies of which are available upon request.

Eileen Poiani of St. Peter's College in New Jersey has worked at the national level on issues involving women in mathematics. She was interested to learn from [redacted] that NSA has many highly qualified women among its professional mathematicians, and asked if some of them would be willing to participate in her projects.

P.L. 86-36

At the NSA Conference, Askey asked me to look up Nevai of Ohio State. He was the organizer of a special session. I asked Nevai about using orthogonal polynomials to approximate tails of distributions. He asked me to send him my paper. Askey and I talked several times. At the NSA Conference he had argued for orthogonal polynomials as the solution to estimating extreme tails. The three-term recursion allows one to find orthogonal polynomials using the metric from the quadratic form dictated by the given moments. In theory, if the moments determine the distribution, the set of orthogonal polynomials determines the distribution. The practical utility for tail estimation is unclear.

Lax had told [redacted] at the NSA Conference that mathematicians have new and better ways of doing extreme tail approximation that statisticians have not yet learned. Accordingly, I cornered Lax and asked him what methods he had in mind. Lax thinks he has a clever way of finding the roots of orthogonal polynomials without the expense of generating the polynomials. (See Diaconis' talk.)

DR. GRAHAM'S ADDRESS

President's Science Advisor and Director of the Office of Scientific and Technical Policy (OSTP), W. R. Graham, stressed the need for educational reform, interdisciplinary cooperation, and lobbying for more government funding. The audience was tiny, which may or may not reflect the popularity of the US government at this conference. (It certainly reflected the availability of free beer at an Academic Press dinner held at the same time!)

Graham spoke first on government investment in mathematics, stating that the government is used to people lobbying for support and feels no need to force its money on people. He stated that support to mathematics is based on the premise it is crucial to future economic and military security. DoD is finally willing to give independent support for academic research, a healthy sign. Mathematics should involve itself in interdisciplinary efforts that prove its value.

In Graham's view, the health of mathematics depends on finding ways to apply it to the benefit of the non-mathematical public. He believes mathematics teaching in high school is poor. We expect little of our schools and students, so we cannot hope to compete with foreigners. The Mathematics Science Education Board should help. Demographics will be an increasing problem in getting enough good teachers [and Agency employees!] Decentralization may make reform difficult.

RECRUITING

The Agency recruiting effort was apparently quite successful. About thirty people were interviewed. This included most of the people who seemed to be good prospects. Of course, only time will tell which of these people will end up on board.

MATHEMATICAL HIGH POINTS

A short course on Moments in Mathematics included, among other things, the following:

- Diaconis' work on Wyner's encryption method for speech over telephone lines and his ideas on attempts to extend Chebyshev's bounds.

- Kailath's talk on speech synthesis, lattice filters, fast methods of finding Cholesky and QR factorizations, transmission line theory, and a parallel algorithm for decoding certain codes.

Of the other lectures given, the following were of particular interest:

- An interesting talk on radar by J. Michael Baden & Marvin N. Cohen of Georgia Tech.

- McEliece on neural networks. They can be used in theory to find local minima of NP-complete problems and as storage devices.

- A talk by Durrett on modeling for a variety of growth and decay situations. One wants parameter values for which a process dies out or lives.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

- Talks by K. S. McCurley on sieving the positive integers by primes, by Tapia on an unsuccessful attempt to use Karmarkar's methods to do quadratic programming, and by R. A. Mollin on the class number of certain real quadratic fields.

SOME DETAILS

Richard Durrett, Cornell Univ., ***Crab Grass, Measles, and Gypsy Moths: An Introduction to Modern Probability***. A preprint of Durrett's paper is available. The subject is five different models for interacting particle systems. One asks in each case under what parameter settings the phenomenon survives forever or dies out.

1) The Oriented Percolation Model.

2) Richardson's Model (Sites become occupied with a probability depending on the number of occupied neighbors.)

3) The Measles Contagion or Forest Fire Model (similar to no. 2, except there are three states, tree burnt, whole, or on fire.)

4) The Gypsy Moth Spread Model (similar to no. 1 except that time is a continuum).

5) The Crabgrass Spread Model on a lawn $(Z/M)^d$, where M is a large integer.

J. Michael Baden & Marvin N. Cohen, Georgia Tech., ***An Application of Undergraduate Mathematics Yielding Interesting Results in Radar Research.*** Cohen gave an introduction to radar with applications to ground mapping, surveillance, tracking, and signature acquisition. Long pulses give long range but weak resolution. Pulse compression involves coding the long pulse to improve resolution. Cohen explained filtering to handle sidelobes caused by correlations out of synch. One wants to minimize both the integrated sidelobe level and the peak sidelobe.

There are 8 Barker codes that have optimal sidelobes. But it is now known there are no Barker codes of length more than 13 and less than about 10000. One wants codes of length in the thousands. One can combine Barker codes to obtain longer codes. Also, there are Golay pairs. They are ideal, except that movement of the target or any sort of instability kills them.

Baden uses a method involving mismatched filters to reduce the sidelobe. The filter depends on the signal. In practice, one designs the filter with a sample of the signal, and assumes this will be close to optimal. One has to solve a linear system, which by a physical argument is invertible. Baden would like a mathematical reason why the system can be solved. Mismatched filters do much better than the alternatives, especially as the filter gets longer. Charts allow one to select the proper filter length to get the desired sidelobe characteristics.

Marc Culler, Univ. Illinois Chicago, ***Free groups, Trees, and their Automorphisms.*** This talk on geometric group theory included a reference to work of Ken Moss. Given a free group F, one tries to describe the outer automorphisms OUT(F). On the other hand, following Thurston's work, one seeks to characterize the points at infinity needed to compactify a topological space. The connection between these two problems is a generalization of the concept of tree.

Robert J. McEliece, California Inst. of Technology, ***The Capacity of Neural Networks.*** This is joint work with Posner, Rodemich, and Venkatesan. Neural networks are arrays modeled on the brain. Each neuron has a binary state (firing or not firing). It decides to change state on the basis of the sum of inputs from all the neurons to which it is connected. There is a threshold function for computing the new state depending on a symmetric matrix T. The initial state is called a prompt. At any given time, the node most urgently wanting to change is the one that changes (with some tie-breaking procedure). If the prompt is [+-+-++], and we multiply this by matrix T and obtain for example the vector [-1 5 -1 5 3 3], then nodes 1,2,3,4 want to change sign, while nodes 5 and 6 do not. The ones most urgently wanting to change are 2 and 4, so one of them is selected. If T is symmetric with zeros on the diagonal, this process will always converge to a fixed point, a local minimum of energy. In theory one can build a neural network to find local minima of NP-complete problems, such as the Traveling Salesman Problem. McEliece described how a network can be used as a storage device. One designs a neural network with matrix T chosen so that the words to be remembered are fixed points. However, there may be other fixed points to complicate matters, and other problems may arise. Neural networks are easy to build and to update.

R. A. Tapia & J. E. Dennis, Rice, & A. M. Morshedi, Shell Development, ***Polynomial-Time***

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

Quadratic Programming based on Karmarkar's Linear Programming Approach. Ye & Tse and Kapoor & Vaidya tried in 1986 to use Karmarkar's methods for QP. Their efforts are unsatisfactory for different reasons. The authors have tried again, also with unsatisfactory results, but for a bizarre reason.

R. A. Mollin, Univ. of Calgary, ***Class number of real quadratic fields.*** Mollin provides sufficient conditions for the non-triviality of the class numbers of certain real quadratic fields.

K. S. McCurley, USC, & D. A. Goldston, San Jose St., ***Sieving the Positive Integers by Large Primes.*** If Q is a set of primes, let $\psi(x,y,Q)$ be $\#\{n \mid n \leq x$ and $(p|n, p \in Q) \Rightarrow p \leq y\}$. The authors prove an estimate for $\psi(x,y,Q)$ in terms of a generalized Dickman function, extending work of Hildebrand. This yields an asymptotic estimate for $\psi(x,y,Q)$. One result is that removing small prime factors in sieving has less than the expected effect.

SHORT COURSE ON MOMENTS METHODS

I attended a three-day short course on Moments in Mathematics. In general, the experts at the course tended to approach moments from a function-analytic point of view and had relatively little experience with statistics. The course served as a general survey. I particularly liked Kailath's applications-oriented talk.

Henry J. Landau, Bell Labs, ***The Classical Background.*** Landau gave a survey of moments problems and applications, beginning with the Hamburger Moment Problem (find a measure on the real line with a given set of moments and determine if the measure is unique), the Truncated Moment Problem (only 2n moments given), and the Trigonometric Moment Problem (the equivalent existence problem but with complex moments on a circle - uniqueness following by Fourier transform theory.) A necessary condition for existence of a solution to the Hamburger Moment Problem is that a certain quadratic form be positive semi-definite. In this case, it defines a scalar product for polynomials, and so a family of polynomials orthogonal with respect to this product. He showed positive semi-definiteness is sufficient for existence. Landau discussed generalizations and applications.

J. H. B. Kemperman, Rutgers, ***Geometry of the Moment Problem.*** Given a set of measures, we can map them to points in n-space by taking each measure to the point (the "moment point") with coordinates the given n moments. For measures on an arbitrary measurable space, more general geometric constructs can be considered. Given a finite number of moments, one wishes to describe geometrically the convex set M of all measures having these moments, or at least to give accurate bounds for the integrals of particular functions as the measure ranges over M. Or one may require that some of the moments are not prescribed exactly, but only fall within given bounds, or on a line in n-space. Or, given a set A, fix moments and ask for the largest or smallest mass for A consistent with the moments. Such problems are conceptually simple but hard.

Donald Sarason, UC-Berkeley, ***Moment Problems and Operators in Hilbert Space.*** The connections between classical moments problems and the theory of operators in Hilbert space were recognized early on. Sarason described some of these connections. For example a one-sided version of the trigonometric moment problem, the so-called Nehari Moment Problem, is related to the theory of Hankel operators. A proof of the sufficiency of the positive semi-definiteness of the Hankel matrix for the Hamburger Problem follows from the Spectral Theorem for Self-Adjoint Operators. One can give function-theoretic conditions for the solution to be unique.

Thomas Kailath, Stanford, ***Signal Processing Applications of Some Moments Problems.*** Trigonometric moment problems are connected with positive definite matrices, orthogonal polynomials, and classical function theory. These subjects all are related in turn to a variety of signals processing problems: linear prediction, inverse scattering, digital filtering, etc. Kailath illustrated the interplay between moments problems and signals theory. Starting with linear predictive coding methods as applied in speech synthesis (the way modern American toys have learned to speak!), he described the role of Szego polynomials in providing a nice hardware implementation.

The issue of parallel implementation of image processing brings in an algorithm of Schur. This leads to a new class of digital filters called lattice filters that have excellent robustness to finite precision implementations.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

An offshoot is a fast method for finding Cholesky and QR factorizations of Toeplitz matrices. Other applications are to transmission line theory, layer-peeling algorithms for inverse scattering, and parallel algorithms for decoding Reed-Solomon and BCH codes.

Christian Berg, Univ. Copenhagen, Denmark, ***The Multidimensional Moment Problem and Semigroups.*** The 2-dimensional moment problem consists in finding necessary and sufficient conditions for a sequence s(m,n) m,n = 0,1,... to be a moment sequence for a non-negative measure on the real plane. More generally, in the n-dimensional case, one would like to characterize moment sequences among all sequences, characterize which are determinate, and give a complete description of the set of measures with a given indeterminate moment sequence. The theory of moments may be viewed as harmonic analysis on semigroups.

Persi Diaconis, Stanford, ***Moment Problems in Probability and Statistics.*** Statisticians use moment estimators as basic in applied work. For example, Diaconis said that the distribution of traces on the n-dimensional orthogonal group has the same first 2n+1 moments as the standard normal distribution. In the application, which was a proposal by Aaron Wyner of Bell Labs to encrypt speech for phone lines using random orthogonal matrices, this was bad news. Diaconis and his co-workers were trying to approximate Haar measure for the orthogonal group using iteration of random reflections. A reflection fixes a hyperplane, so log n reflections will fix too much and the trace of the iterated operator will be too large. One needs n log n reflections to get the trace right.

Diaconis mentioned Chebyshev's bounds on a distribution with the same first n moments as the standard normal distribution. There is a bound on the error, but it is attained by discrete distributions. If one looks at smooth distributions, the bound is very poor. Diaconis would like more work on what can be said with smoothness assumptions. I mentioned that robustness considerations both on the moments being equal and on smoothness must be studied. What if one drops normal? Diaconis and I have both been trying to get people to work on such problems.

Diaconis said that the modern approach to bounding variability among distributions with a prescribed n moments leads to numerical determination of the zeros of the associated orthogonal polynomials. This is feasible for a small number of moments, but is quite difficult in general. Are these bounds on all distributions with a fixed n moments useful? Probably the smoothness problems mentioned above occur generally.

Diaconis discussed Hausdorff's Moment Theorem which addresses the question: when is a sequence the moment sequence for a distribution on the interval [0,1] and De Finetti Exchangeability. Roughly, De Finetti's theorem says that *a distribution on sequence space is exchangeable if and only if it is a mixture of Bernoullis in a generalized sense.* This theorem is equivalent to Hausdorff's Moment Theorem. One can relate extensions of de Finetti's theorem to moment problems and so generate new problems.

MISCELLANEOUS

Many exhibitors were present and distributing literature. Literature and demonstrations on word processing were particularly evident. Mike Spivak showed his own commitment to TEX by typing people's equations in great numbers.

Among conferences advertised was the First Canadian Number Theory Society Conference, at Banff, April 17-30, 1988. A tentative list of speakers includes Erdös, Guy, H. Lenstra, Pomerance, Ribenboim, Selfridge, Washington, H. Williams, and Zassenhaus.

The AMS awarded Steele Prizes to Donald Knuth (for his book), Rudolf Kalman (for papers on filtering and linear dynamical systems), and Saunders MacLane (for cumulative influence, especially on homological and categorical algebra.) The Cole Prize in Number Theory was shared by Benedict Gross, Dorian Goldfeld, and Don Zagier for work on the class number problem for imaginary quadratic fields. As for MAA awards, the Chauvenet Prize went to J. H. Wilkinson, the Allendoerfer Awards to Bart Braden and Sol Stahl, the Ford Awards to Jeffrey C. Lagarias and M. E. Taylor, and the Polya Award to P. J. Davis. □

Editor's Note: We just learned that the resolutions passed during the AMS business meeting were subsequently ruled out of order by the General Council. It is expected that there will be a referendum on the motions after January 1988.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4010012

"NSA" PUZZLE

P.L. 86-36

by [redacted] T12

The occurrence of "NSA" as a letter sequence in English words is rather uncommon. Some of the rare examples are shown below. Fill in the blanks to reconstruct the "NSA" words defined.

A. Crazy — n s a _ _

B. "Land of Opportunity" _ _ _ _ n s a _

C. Lacking sodium chloride _ n s a _ _ _ _

D. Pay for damages _ _ _ _ _ n s a _ _

E. Miniature tree _ _ n s a _

F. Unable to be satisfied _ n s a _ _ _ _ _ _

G. Across the ocean _ _ _ n s a _ _ _ _ _ _ _

H. Middle Eastern inn _ _ _ _ _ _ n s a _ _

I. Unhealthful (as a climate) _ n s a _ _ _ _ _ _ _ _

J. Not spoken _ n s a _ _

K. Search thoroughly _ _ n s a _ _

L. Deny or contradict _ _ _ n s a _

M. Not paid regularly _ n s a _ _ _ _ _ _

N. Relationship by descent from a common ancestor _ _ n s a _ _ _ _ _ _ _ _

O. Unclean _ n s a _ _ _ _ _ _

P. Result of a bank visit _ _ _ n s a _ _ _ _ _

Q. Disagreeable or disgusting _ n s a _ _ _ _

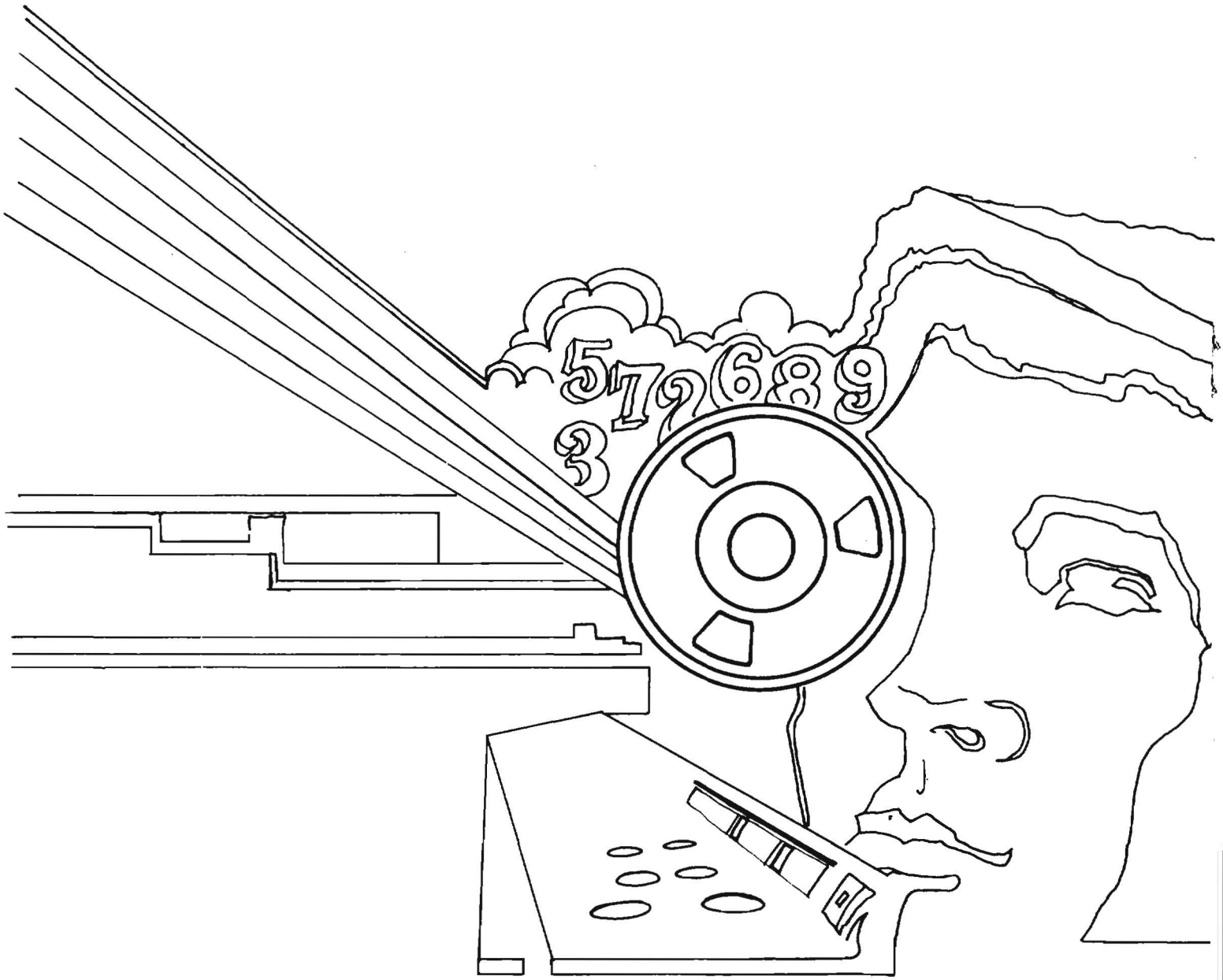
R. Type of roof _ _ n s a _ _

S. Sail on a square-rigged vessel _ _ _ n s a _ _

T. Able to combine with other substances _ n s a _ _ _ _ _ _ _

~~FOR OFFICIAL USE ONLY~~

Y16


5 7 2 6 8 9
3