~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JUN-AUG 1985

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~DECLASSIFY ON: Originating~~ ~~quired~~

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XII, Nos. 6-8 ..... June-August 1985

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 Subscriptions or Change of Address
send name and organization to:
P14

P.L. 86-36

P.L. 86-36

EDITORIAL

Analysts in NSA have an opportunity to share their views and experiences with others by writing for one of the several periodicals published in the Agency.

One of them is CRYPTOLOG. It is specifically intended for informal exchanges among analysts on subjects of interest to them. The editorial blue pencil is lightly applied, and only in the interest of clarity ... it's up to you to sustain the readers' interest and to put your ideas across persuasively.

For assistance, advice, or just plain aid and comfort, you may call on any of the editors; it need not be the one on your subject.

As for anonymity, we follow the standard etiquette of most publications: We will honor the author's request to remain anonymous, (we will even provide a nom de guerre for those who might want one) but the identity of the author must be made known to the Editor. Anonymous contributions (that is, lacking identification of the author) may as well be written in invisible ink ... we throw them out unread.

Another point of etiquette that authors must observe is about multiple submissions. If you send your article to more than one publication, you must so state.

Now for a few tips to ensure early consideration:

** The subject should be related in some way to our business. Unclassified term papers seldom fill the bill.*

** The article should be shorter rather than longer. A readers' survey showed that long articles are not read.*

** The text and illustrations should be of reproducible quality.*

** Every paragraph and illustration should be appropriately classified.*

** Hard copies of articles prepared on word processors should be accompanied by the mag card or floppy. (We send it to the Data Conversion Center where it is transformed to an 860 floppy, and then we convert that to an 8010 floppy.) Be sure to state what equipment and what software you used, and the operating system in the case of a pc.*

** If you submit a contribution via electronic mail, notify us by some other medium that you are doing so. (There's slippage every now and then.)*

** If you're going off on a field assignment or extended training or if you are retiring, designate someone who can act as your literary executor.*

** Label every submission with your full name, organization, and secure phone.*

SECRET

NSA'S INITIATIVE ON SECURE VOICE (U)

P.L. 86-36

[redacted]

(U) The Soviet Union and other hostile governments can intercept and exploit, with ease and impunity, many U.S. telecommunications in the continental United States and around the world. Classified and sensitive communications over unsecured telephone systems alone represent such a lucrative and easy source of intelligence that NSA has undertaken a bold new approach to counter this threat.

(U) Each of NSA's past efforts to develop and distribute COMSEC equipments to the field has taken many years to complete. To reduce this time significantly NSA decided to tap the knowledge and resources of major commercial manufacturers of telecommunications equipment in a program called The Future Secure Voice System (FSVS) whereby NSA provides the cryptologic expertise and contractors provide technical, manufacturing, and marketing know-how. The goal is to design and produce a secure telephone the size of a conventional office deskset which will plug into a modular jack, cost less than $2,000, and be simple to operate.

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

EXTENT OF THE THREAT

(S-CCO) Unsecured telephone conversations can be easily exploited by hostile intelligence-gathering activities to reveal governmental, military, and industrial secrets and technology. That is because communications over commercial telephone systems, especially long distance, are likely to be transmitted via microwave or satellite which are particularly easy to intercept; all it takes is equipment costing about $25,000, small enough to fill the back of a station wagon.

[redacted]

(S) Moreover, mission-essential, classified information is sometimes discussed over unsecure telephones simply because secure communications are unavailable. Unclassified but sensitive technological data also pass over the telephone system daily. As a recent National COMSEC Committee Biennial Report points out, "the industrial base which produces the nation's most advanced military hardware and develops its most sensitive technology is almost completely without a secure communications capability. Critical secrets are lost before the sensitive systems and technologies they represent can be fielded by military or other government users."

(U) The unsecured telephone has been determined to be the most lucrative source of classified and sensitive information available to unauthorized recipients. To counter this vulnerability, President Reagan recently signed National Security Decision Directive (NSDD) 145, which directs that all U.S. Government systems carrying classified information be secured, including telephone.

(U) NSDD-145 requires that NSA, as the new National Manager for Telecommunications Systems Security, provide a secure communications capability for as many as 500,000 users beginning in 1987. The FSVS program has been conceived to help implement this directive.

PRESENT SECURE TELEPHONE SERVICE

(C) The only DoD-wide, secure telephone system available today is AUTOSEVOCOM, which serves about 2,500 locations around the world. This system, however, secures only a small fraction of the total telephone conversations of the DoD, and much of the equipment is outdated and provides poor voice quality. Under the recently implemented AUTOSEVOCOM Life Cycle Extension Program (ALCEP), older HY-2/KG-13 equipment is being replaced by newer VINSON devices, which will update the system and improve voice quality. The total AUTOSEVOCOM community will, however, remain small.

(C) NSA's Secure Telephone Units (STU-II and STU-IIM) are also being procured by military departments and the civil sector. Over the next five years the total number of STU-II and STU-IIM units should reach approximately 14,000 units, which is only a small portion of the half-million or so of the secure telephones needed. Because of their relatively high cost ($12-25,000) and their dependence on the Bellfield Key Distribution Centers (KDCs) each of which can service only a limited number of subscribers, these units cannot be distributed to the field in large

quantities. KDCs act as centralized points for electronically distributing key, a function necessary in communications security.

STU-III FAMILY OF TERMINALS

(U) With a half million or more potential customers to satisfy, NSA realized there will be a variety of user requirements. A family of telephone terminals rather than a single type will therefore be developed to satisfy the diversity. This family of equipments has been designated STU-III or Low Cost Terminal (LCT).

(U) Military planners have stated a requirement for the STU-III to interoperate directly with existing STU-II units. This is being satisfied with the STU-III Command & Control (C^2) version, designated KY-77. The C^2 terminal will meet environmental requirements for mobile radio telephones and is planned for limited military and civilian government applications. It will be slightly more expensive than the other members of the STU-III family, and is being developed by RCA on a separate contract. The KY-77 should be available early in 1987.

(U) Of the non-military users of STU-III, some handle classified information and others handle unclassified but national security-related information. Classified user requirements will be satisfied by a Type I LCT, while unclassified users will be limited to Type II terminals. An example of a Type I application is the securing of conversations between NSA and contractors working on classified NSA projects. Typical Type II applications include the protection of proprietary information such as financial, organizational, marketing, and technical data.

(U) Another version of the LCT being conceived is a cellular radio telephone model. This unit, compatible with other LCTs and regular, unsecured telephones will satisfy secure mobile requirements.

(U) Members of the STU-III family will look and act much like conventional telephone desksets. In fact, an LCT will interoperate easily with a regular telephone for unsecured communications. Secure operations between STU-IIIs will require only a few extra steps by the users. The terminals themselves will include modern telephone features like repertory dialing, and will offer a light-emitting diode (LED) or liquid crystal display (LCD). The display will indicate the identity and security clearance level of the distant end terminal, and will help guide users through STU-III operating procedures.

PROGRAM STRATEGY

(U) In the Spring of 1984 NSA asked five major telecommunications contractors (AT&T, ITT, GTE, RCA, and Motorola) to define a concept for the STU-III/LCT and the attendant system necessary to key and support it. This concept definition phase lasted six months.

(U) NSA's program strategy was to select three of the vendors to produce telephones, and one contractor to develpp a system responsible for such things as key management. The selection process is now complete, and the system contract has been awarded to GTE, while AT&T, RCA, and Motorola have been contracted to produce the phones. This parallel acquisition strategy is necessary to achieve NSA's goal of initial delivery in early 1987.

COMSEC DOCTRINE

(U) Physical handling requirements for such a large quantity of COMSEC devices are a major concern. COMSEC doctrine is being rethought in order to lessen constraints and make COMSEC more desirable to the user community. Older security doctrine dictated the handling of cryptographic equipment according to equipment type. STU-III equipment, however, will be governed by new doctrine, which bases the amount of required protection on the specific application of the device. For instance, a STU-III located within the NSA compound will require less stringent control than a unit housed overseas, where foreign nationals may have easy access to it.

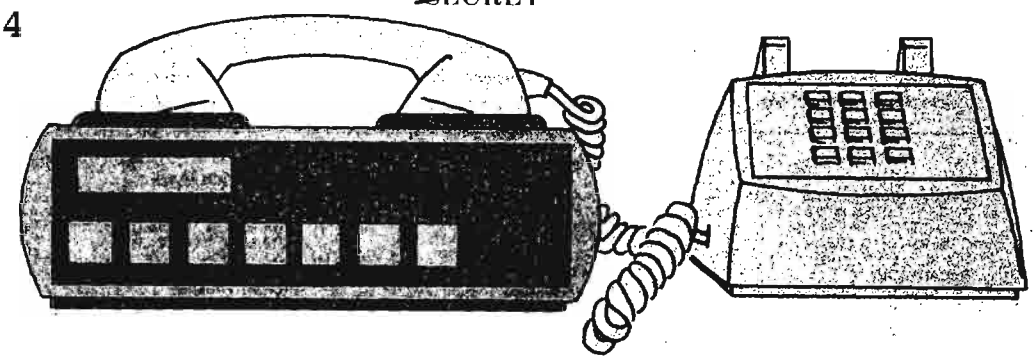
(U) In December, 1984, NSA commissioned A.D. Little Company to complete a market survey to determine the size of the potential market for STU-IIIs and to establish a priority list of user preferences and demands. According to the company's preliminary report, the number one requirement expressed by potential users in both Government and industry is that the units be unclassified when unattended. This condition presents a problem, however, since these terminals are to be high-grade cryptographic devices which normally require special handling. A device called a crypto-ignition key (CIK) will therefore be implemented to help solve that problem.

(U) The security of U.S. COMSEC equipment depends on protecting the key which is instrumental in determining the pattern of ones and zeros, called the key stream, produced by a key generator or cryptologic. The CIK is a removable device, small enough to fit in a shirt pocket, that contains a portion of the key; the other portion resides in the STU-III. A keyed STU-III is therefore sanitized by unplugging and removing the CIK, and the sanitized phone becomes unclassified and can be left unattended. Controls on the CIK will depend on specific applications, but in some cases simply locking the device in a desk drawer or taking it home will be sufficient.

(S) Because STU-IIIs will be widely distributed, it must be assumed that U.S. adversaries will obtain some of the units and attempt reverse engineering in order to recover the cryptologic. To counter this potential threat, NSA has decided on a special chip coating as a way of preventing the reverse engineering of cryptographic chips within the terminals. NSA engineers are confident that this protection will effectively thwart the recovery of information from the circuitry or memory of the chip sets.

KEYING SCHEME

(U) A major effort is required to provide keying material to COMSEC equipment in the field. In most cases, NSA produces the key in some hard copy form like key tape, key card, or key list, and then distributes the key among many users. Some newer equipments, like the STU-II, employ remote keying which reduces NSA's burden significantly. These remote keying schemes, however, generally depend on a KDC or other central point to distribute key electronically to remote users. There are, however, physical limitations on the number of users the KDCs



can support. Therefore, if a half million or more LCTs must be supported, a new keying method is necessary.

~~(C)~~ The new method is called FIREFLY II. This is a breakthrough in key distribution technology in that it will eliminate the need for a KDC by allowing each STU-III to generate and securely exchange key with other STU-IIIs. The calling and receiving terminals themselves generate random components which are then securely exchanged, combined, and used by both terminals on a session or per-call basis. Session keys enhance the security of the system by eliminating back-traffic vulnerability, and the entire process of generating and exchanging random components takes less than 12 seconds.

~~(C)~~ Added benefits of FIREFLY II include positive authentication of distant end terminals, and very long cryptoperiods. (A cryptoperiod is the length of time a particular key may be used before it is replaced.) Although each STU-III generates and exchanges key each time it is used securely, there are also keys which reside within each terminal which must be replaced periodically, every one to three years. This replacement will be as simple as placing a call to a key management center, and receiving new key securely over the telephone line.

APPLICATIONS OF THE STU-IIIs

~~(C)~~ NSA's Deputy Director for Telecommunications has expressed support for the eventual replacement of some NSA black telephones with STU-IIIs. The FSVS initiative, in fact, seeks to install 500,000 secure phones in the Department of Defense, Civil Government sectors, and defense contractors. That number grows considerably when other potential LCT customers are included. Financial institutions, academics doing Government research, and any company performing high-tech research and development that could be transferred to an enemy's military or security systems must be considered prime LCT candidates.

(U) Only a preliminary report of A.D. Little's market survey has been completed to date, but NSA believes that private sector interest in an inexpensive, secure telephone could eventually increase the market to 1.1 million. Independent market surveys performed by some of the bidding contractors indicate an even larger potential market. An RCA-financed study established the market size as over 1.6 million, while other contractor studies indicate a potential private sector market demand by 1990 as high as 2.6 million. The higher numbers reflect the private sector's interest in acquiring secure telephones to protect against loss of proprietary information.

(U) NSA will permit direct, controlled sales of LCTs by the contractors to authorized purchasers. This will allow the vendors to have a direct effect on the size of their market. Clearly, LCT vendors could benefit dramatically from the production, marketing and sale of secure phones. Even if NSA's initial estimate of 500,000 units is inaccurate by 50%, it still means a market of 250,000 phones priced at around $2,000 each, for an estimated total market of $500 million over the next five years. If the private sector market pans out and over a million units are sold, LCT vendors stand to profit handsomely.

(U) Parallel production by three vendors should increase the number of units produced, which will in turn bring down unit cost. The benefits of low cost and high quantity to NSA's COMSEC effort is that many telephone conversations containing classified or sensitive data will be secured, and unaccessible to Soviet and other hostile intelligence activities.

SUMMARY

(U) The huge amount of classified and sensitive information the U.S. is giving away through unsecured telephone communications must be stopped and stopped soon. Older methods of developing and implementing COMSEC are too time-consuming to be effective quickly enough. NSA's FSVS program has therefore been established as a new approach to meeting this COMSEC challenge.

(U) The STU-III family of secure telephone equipment is now in contract, with initial distribution to the field planned for April, 1987. It will provide advantages in size, acquisition and life cycle cost, security and performance over current secure voice equipment, and meet a broad variety of needs.

(U) Various STU-III models will provide compatibility with conventional office telephone systems, military strategic command and control requirements, and conventional and cellular mobile radio telephone systems. Most significant is the very scale of the program, with quantities ultimately expected to exceed half a million units.

(U) All aspects of NSA's Future Secure Voice initiative add up to an strong program to protect the voice communications of the U.S. If this effort is successful, and the contractors and NSA believe it will be, we can truly button up U.S. voice communications by the end of this decade, and, at the same time, deal the Soviets a severe blow. □

P.L. 86-36

TELEPHONE SECURITY, 1918

Extract from Confidential orders to 1st Lt. (Chaplain) John McDowell Alexander Lacy, October 12, 1918.

1. Having reported at this office, this date, for transportation in compliance with order Headquarters, Port of Embarkation, Hoboken N.J. or from Navy Department, you will report at Officer's Gangway, Vessel No ..*56*.. Pier No ..*59*.. North River, Foot of West ..*18th*.. Street, New York City, at ..*4*.. ~~A.M.~~ P.M. ..*Oct 16*..1918.

3. You are directed not to visit pier to which you have been assigned before date of embarkation except for the purpose of delivering your baggage. You will then go only to the Baggage Room, and under no circumstances wander about piers or go near vessel.

8. No information will be given by telephone.

9. THIS INFORMATION IS STRICTLY CONFIDENTIAL.

Courtesy of [redacted] *S052, grandson of Chaplain Lacy*

BULLETIN BOARD

FOR DATA BASE ADMINISTRATORS

~~(FOUO)~~ The Computer Record Format (CRF). form H3173C, has been revised. It is now on the new standard paper size, 8½x11, to be consistent with the Computer Services Work Request form, H3173, which it accompanies. The CRF is a vehicle for documenting files; it is the official repository for information about the individual file(s) and record formats, subordinated to a particular file or data base, which are going to reside on T-controlled resources, such as CARILLON, CARONA, HOLDER, METEOR, PLATFORM, WINDMILL.

~~(FOUO)~~ The National Data Standards Center, P13D, recommends that data base administrators use this form to document all files created under their cognizance, including those entered experimentally or provisionally on micros or terminal subsystems. Then, when the programmer is sud-denly transferred, you'll have some idea about what those strange files are. The failure to document small, private files which go on to become big, shared files is becoming a serious problem in the Agency.

(U) The new forms should be available in Supply by the time you read this.

DO YOU WRITE AND EDIT IN YOUR JOB?

(U) If you do a significant amount of writing and/or editing in your job and do not hold a COSC as an editor/writer, please make yourself known to [redacted] T54, SAB 2, Door 3, 972-2355s

CALL FOR CA TERMS

~~(C)~~ The SIGINT Terminology Group is compiling an on-line database of cryptanalysis terms and definitions. Initial input has been drawn from the following sources: *Military Cryptanalytics II*, Lambros D. Callimahos, October 1959; *Basic Cryptologic Glossary*, P1, 1971; *NSA Technical Journal*; *CRYPTOLOG*; [redacted] Suggestions for additional sources are solicited. Please forward your submissions to [redacted] P13D, 968-8162s.

~~(FOUO)~~ The database now contains about 1600 terms and definitions. When the total reaches 2,000-2,500, it will be reviewed by a panel of experts appointed by the chiefs of key components.

SUGGEST-A-BOOK

(U) The NSA Library is soliciting suggestions for books and periodicals to be purchased for the Library. For each book, provide the following information and send it to T51: Author, Title, ISBN, Price, Publisher, Source of Information, and your name, organization and telephone number. It would be helpful if you also include a review of the book or an ad for it.

GLOSSARY OF MACHINE TERMS

~~(FOUO)~~ Contributions are solicited for the Supplementary Working Aid for Machine Terminology (SWAMT) for the updated edition planned to be published early in 1986, the first since 1981. SWAPT is an informal glossary rather than a standard one, so the less formal style allows for the frequent updates which such a rapidly changing technology demands. The next edition will be printed in both upper and lower case, as it is now being processed on an IBM PC to be printed on a laser printer.

~~(FOUO)~~ Contributions, suggestions and comments may be sent to [redacted] P13D, FANX III, or you may call her on 968-8162s.

FOR PINSETTER USERS ON THE XT OR ASTW

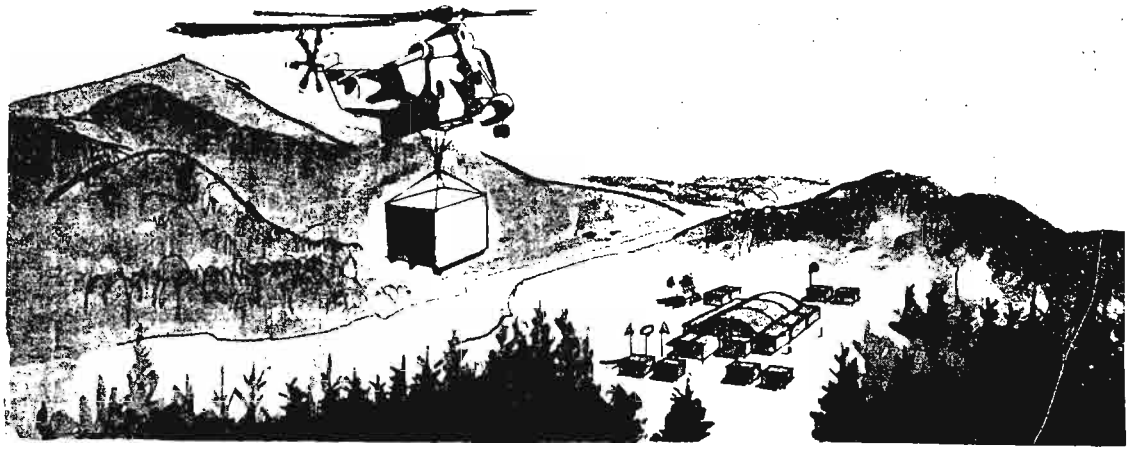
~~(FOUO)~~ A new PINSETTER applications manual, *How to get Started with the IBM PC/XT or ASTW* is now available at the PCIC and P14. It provides helpful hints to new users of the PC/XT or ASTW, whether experienced or not in using the TSS/UNIX version of PINSETTER.

~~(FOUO)~~ For further information or assistance, call [redacted].□

SHOPWORK IV (U)

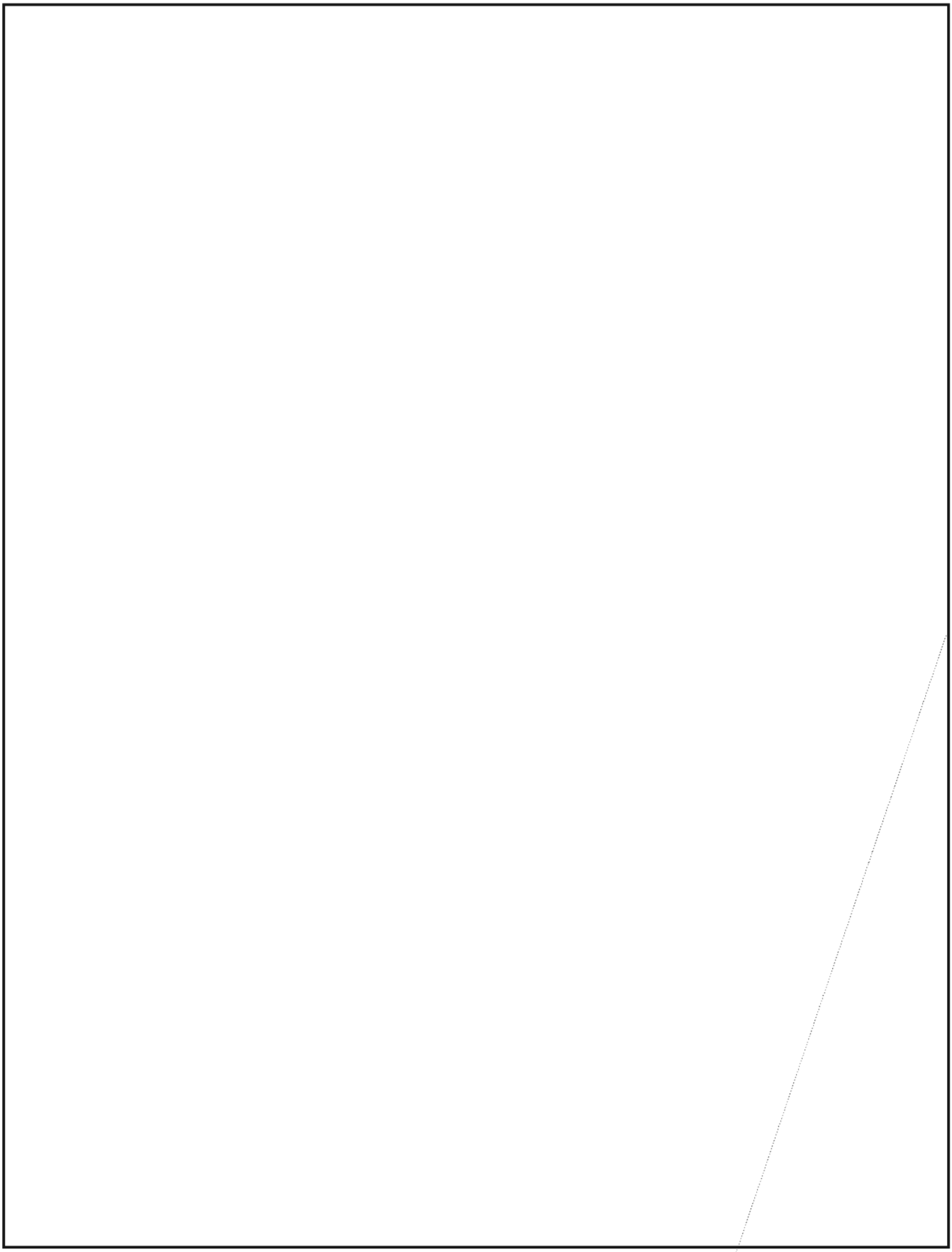
[redacted] *USA, JOCCP*

P.L. 86-36



[redacted]

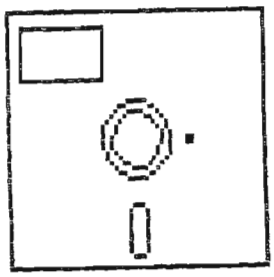
P.L. 86-36
EO 1.4.(c)

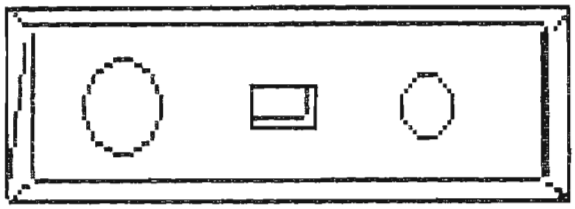


AN APPLICATION OF PINSETTER (U)

[redacted]

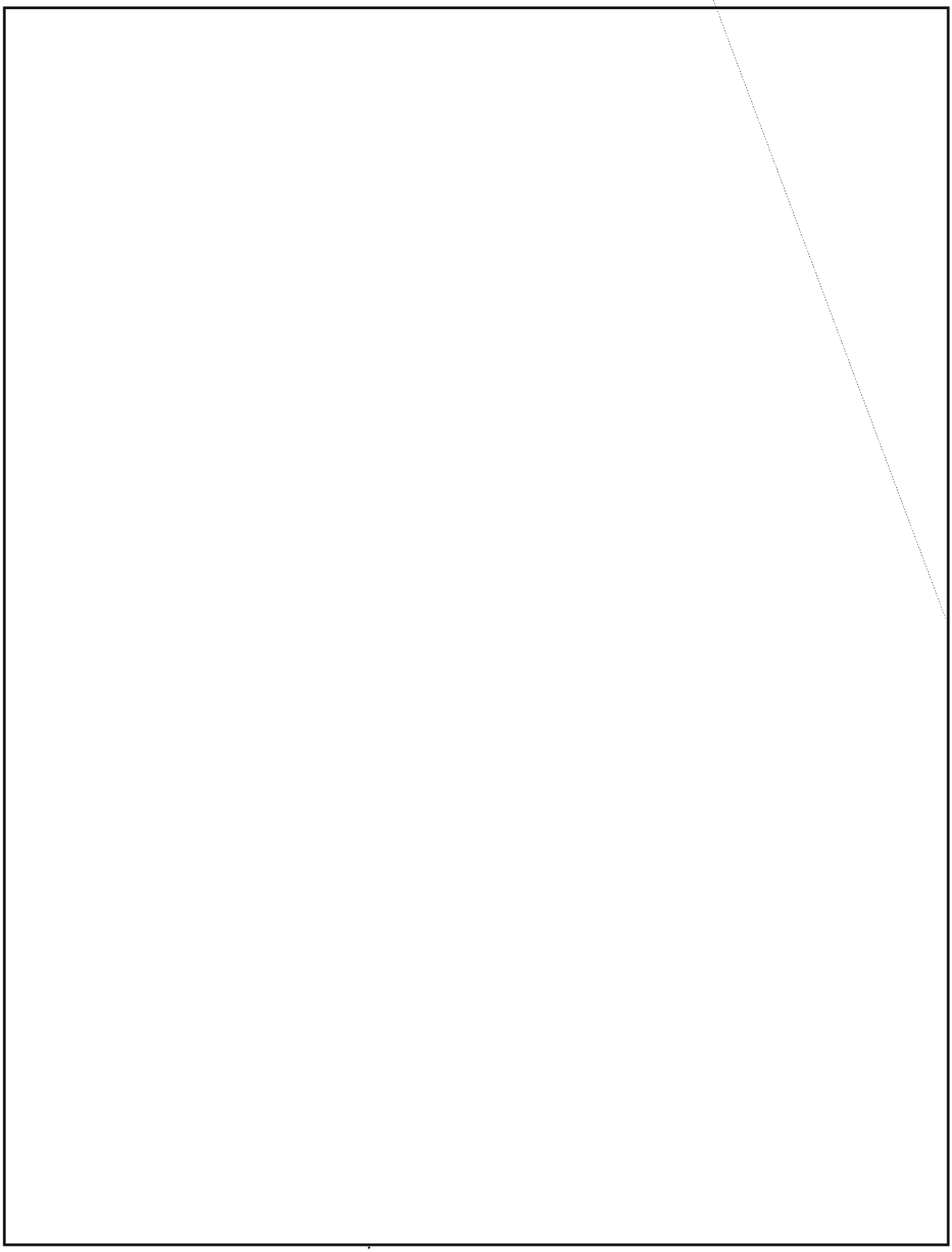
P.L. 86-36



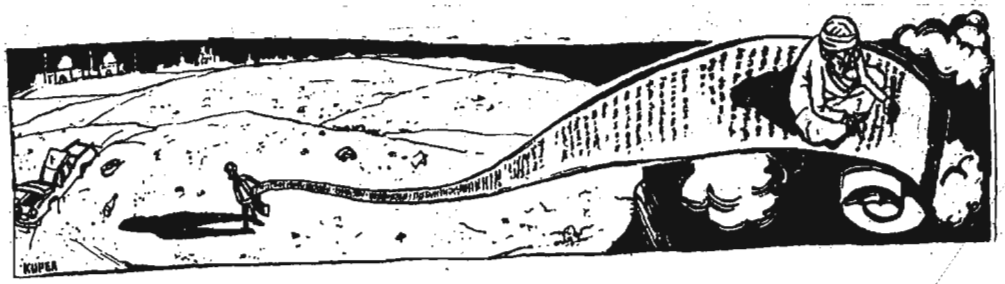


[redacted]

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



VALEDICTORY OF A TRAFFIC ANALYST (U)



[redacted] Ret.

(U) On August 1, 1985 I retired from the National Security Agency after almost 40 years of cryptologic work which included at one time or another most of the things NSA does in the fields of collection, analysis, and SIGINT reporting. I enjoyed every minute of it. I honestly don't believe I could have chosen a more enjoyable or rewarding career. If I had been born rich, Iwould have done traffic analysis for nothing; if I had been independently wealthy, I would have paid the Agency to let me do it. Hang with me for a few minutes of serious discussion about machine processing problems, and I'll share with you a few observations, comments, and recommendations that may contribute to your enjoyment of the profession and perhaps help you to avoid some of the pitfalls that beset the paths I wandered in.

(U) The most important question confronting the profession today is why, from a traffic analyst's viewpoint, data processing systems have not yet produced the Utopia we were led (or stampeded) to expect back in the early 1960's.

(U) In the January-March 1980 CRYPTOLOG, [redacted] correctly sorts working analysts into three categories: loggers, case analysts, and research analysts. He then predicts that automated processing techniques will permit us to eliminate the loggers, and assesses that the research analyst is the one with the bright future because he is concerned with the "why of analysis ... driven by his desire to explain." But every analyst should be saying why, and George's prediction that the logger will become obsolete just hasn't happened, although it should have. Indeed, we now have a new generation of loggers who have even less understanding of traffic analysis than those who preceded them.

(U) After George discusses how analysts are going to have to adapt in order to be productive in a modern (machine oriented) world, he puts his finger squarely on the major problems area, "manageable machine systems that will function as designed." And he goes on to point out,"... our track record for the development of such systems is not impressive."

(U) In the December 1981 CRYPTOLOG [redacted] published an article on machine processing that everyone who claims to be a traffic analyst should have read. Part of what Dale addressed was the problem with keeping competent programmers on the job, and how the traffic analyst could be freed from total dependence on the programmer.

(U) Traffic analysis is basically a very simple art if you are able to keep your mind loose so that you can recognize and exploit whatever the target gives you to work with. This is a fairly easy exercise intellectually, but it is much more difficult to structure your thought processes in order to design a machine processing system that will give you essentially the same versatility. Unfortunately, we have some managers and analysts who have produced processing systems and tried to make the target fit the processing scheme, and I include in this category most of those procedures which were designed to replace a hand log kept by the analysts with a similar log prepared by the machine. The results were predictable. What we have now are logs prepared by machine that in many instances are inferior to those the analyst prepared by hand. And, without the benefit that accrued from working the traffic by hand, today's analyst has even less understanding of the data and may in fact be at a total loss to explain observed anomalies.

~~(C)~~ We can reverse this trend. We need to build on the good decisions we have made with regard to automating data processing for traffic analysis, and we must be willing to discard the bad decisions. What we really need to do now is to get on with developing an expert system that will process automatically all incoming traffic, compare what is observed to a dictionary of stated norms, and send appropriate alert messages to analysts and reporters on trouble spots.

[redacted]

(U) None of this should be difficult. Building and testing dictionaries will be tedious but in the process of doing this, the analyst will be compelled to learn a great deal more about his cases than he now knows, and supervisors will be compelled to work with analysts to a much greater extent than is taking place now. When an expert type system is in place and functional, one of the benefits will be that time will become available for a different and much more meaningful kind of on-the-job training.

~~(S-CCO)~~ We began exploring how to develop an expert system for processing [redacted] just before I retired. I expect initial development to be slow, painful, and frustrating but I do expect the system to "function as designed." What we must have to make it work is a sufficiently confident estimate of our analytic judgments and capabilities to tell the machine

how to do all the dog work for us and then let it do the job. There can be no doubt as to our ability to make the right technical and reporting decisions based on the alert messages because each analyst must understand his responsibilities well enough to have described his case, net, and network norms to his analytic dictionaries.

(U) We will see vastly improved data bases as a side benefit of this kind of processing. If the input data aren't good, the expert system is going to make noise; it will not permit any analyst to do a poor job on editing input data without sounding off.

(U) I am not persuaded that an expert system can be developed and implemented by evolution; probably the best (and certainly the quickest) way to effect such radical changes in the way traffic analysis is accomplished would be to select the right analysts and programmers, charge them with developing an expert system to do traffic analysis on a specific target, and set a deadline of perhaps a year hence for the initial job to be finished. There should be no restrictions as to how the task is to be accomplished, and there should be no arbitrary limitations as to the techniques to be used (e.g. storage of norms for ordinary comparisons should not be made excessively difficult by the intricacies of an existing data base).

(U) There is no question that the agency will deve-lop an expert system at some point in the future; if not for normal traffic analytic functions, then to provide rapid data evaluations for tactical support of military forces. I regret that I will not be here to see it.

(U) Here is the advice I promised earlier.

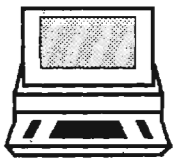
(U) Learn to be persuasive as well as informative in any presentation you make. The best ideas you have aren't worth much if you can't sell them. You cannot depend on decision makers to steer the right course because it is (or appears to you to be) the logical thing to do.

~~(FOUO)~~ Reporting the results of your analysis is part of your job. Learn what the intelligence requirements are for the target you are assigned and relate them directly and specifically to how you work your traffic. If you don't understand what it is that you are supposed to be getting out of the traffic and don't try to find out, you are still a logger and that's all you're ever going to be.

(U) Avoid meetings. I am convinced that many people at the Agency really and truly believe that they are making progress as long as they are talking with each other regardless of whether or not anything is actually being done. I have attended some meetings where the only concrete thing accomplished was an agreement to meet again at some specified date in the future to discuss the same subject. And so help me, they all left happy.

(U) Don't take sinful pride in your own words. If the staff officer who reviews your message or report wants to change your words for his, don't be offended. Staff officers do serve a useful function. If you have treated them with respect in the past, they will often help you get out of trouble.

(U) I finished this article just as my NSA career came to an end. Reading it over, I find a line or two that may be mildly objectionable to one person or another. It was not my intention to offend anyone by my choice of words or by my comments, and if I have given offense, I apologize. This doesn't sound like me but it does sound nice and I think I'll leave it right there. Goodbye, good luck, God bless you all. □



BACK UP YOUR DATA FILES (U)

Norman P. Smith, H215

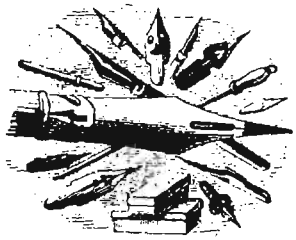
Enough cannot be said about the importance of local backup of data files, especially data being stored in micros. The first thing new users should learn when they receive their own ASTW, PC, or other micro, is how to backup all files and the operating system. The command below will allow all ASTW-PC/IX users to backup their own directories:

find <pathname> -print _ /priv/dump -i -v

where pathname is the complete pathway to the directory being backed up (i.e., /usr/npsmith). Users of TSS and other systems depend upon their systems administrator and the operating systems themselves. Backup copies should probably be made at least every 12 hours, if not every 6 hours, and held for 24 to 48 hours. The rule of thumb for backing up data is to back up your data for the span of time you find acceptable to spend re-creating your work.

Another method to accomplish this on the ASTW is to work directly from floppy disks, where each floppy contains an entire working directory. You then use the MOUNT and UNMOUNT commands to bring up and take down access to the floppy These commands are covered in the ASTW Users' Guide. □

ESCHEW OBFUSCATORY SCRIVENERY, PLEASE (u)



P.L. 86-36

This article is classified ~~SECRET SPOKE~~ in its entirety.

Many operators frequently use the TR NOTE during transcription to elaborate on the traffic, yet few stop to realize just why and for whom they are making the additional entries. When properly employed, the comments contained in the TR NOTE can be of great assistance to those who ultimately read the transcripts, giving them useful information and insights. When abused or misapplied, the TR NOTE adds little of any worth, wastes the transcriber's (and the reader's) time and can be potentially embarrassing for the unit as well as for the U.S. intelligence effort as a whole.

Such notes are brief, informative, professionally executed, and to the point. They add insight, correct mistakes, present information not reflected in the words themselves, and save leg-work for the reader. Contrast them with the following:

Notes such as the latter are most often rendered on mids on the last page of lengthy transcripts of poor readability. They are personal expressions of frustration and exasperation, and do little more than trivialize your work and detract from its overall impact. Please avoid the temptation to indulge. □

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

Reprinted, with permission, from the Summer 1985 issue of VOX TOPICS.

NSA-Crostic No. 62

A. Put away the swords, Heather said

209 219 86 62 189 191 215

B. Ornithogalum thyrsoides (2 wds)

92 76 113 146 155 79 163 88 119 132 24 60 199

143 250 54 4 106 12 176 239

C. Surrey town located above U.S. Marine

142 33 158 130 240 228 145 248 29 9 180

D. Twins age fast at new museum (2 wds)

84 178 202 169 95 127 100 56

E. "And so he mediates, twice near
The tides that wash on old Algier"
(2 wds)

111 14 94 105 247 123 152 131 173 148 201 52 245

226 23 237

F. Head of Metro and DDE visit Douglas

230 154 227 253

G. Get Helen Kennedy.

184 135 89 112 235

H. "Does it hurt?" "___ I laugh." (2 wds)

164 6 91 63 186 223 107 128

I. Hilaire Belloc hero usually has
yellowish hue

26 97 2 224 21 68 65 182

J. Twenty-four hours ago he was a
steady rye drinker

232 77 238 210 137 7 25 241 73

K. Wrapped in the wads of bandage

222 214 225 190 136 171 149

L. Not on hand

37 109 144 67 87 117 213

M. It's the wonderful lather we feel
leads to such a state of perfection
(comp)

20 151 66 121 140 98 203 236 194 254 217 138

N. "Bonnie ———" (2 wds)

133 30 22 17 118 167 251 61 208 177 160 75 81

O. Wearily I left to see my solicitor

104 19 47 166 3 34

P. Disregard

69 179 170 200 206 168

Q. Double checker of a tergiversation

159 147 114 45 42 162 70 141 96 78 244 53 211

15

R. Restive; not asleep (var.)

188 1 231 183 50 27 10 57

S. Worse than a vile sea monster

T. Indian town for two idiots

U. Large ice sheet in Antarctica (var.) (2 wds)

V. To make the stout weed tender, he boiled it longer than anyone else

W. I betrayed him when I saw him swipe a cheddar cheese

X. Smelly seat in church?

Y. Remark directed at Dr. I.Q. (8 wds)

Z. The salamander went home

Z_1. Develop a large state in the mind

212 71 80 41 116 153 83 110 55

229 156 72 46 125 85

49 5 129 122 103 31 187 243 216 40

64 58 174 204 218 197 32 48 101

234 192 99 124 205 195 18

150 39 35 207

233 28 102 242 43 181 172 90 185 161 139 59 82

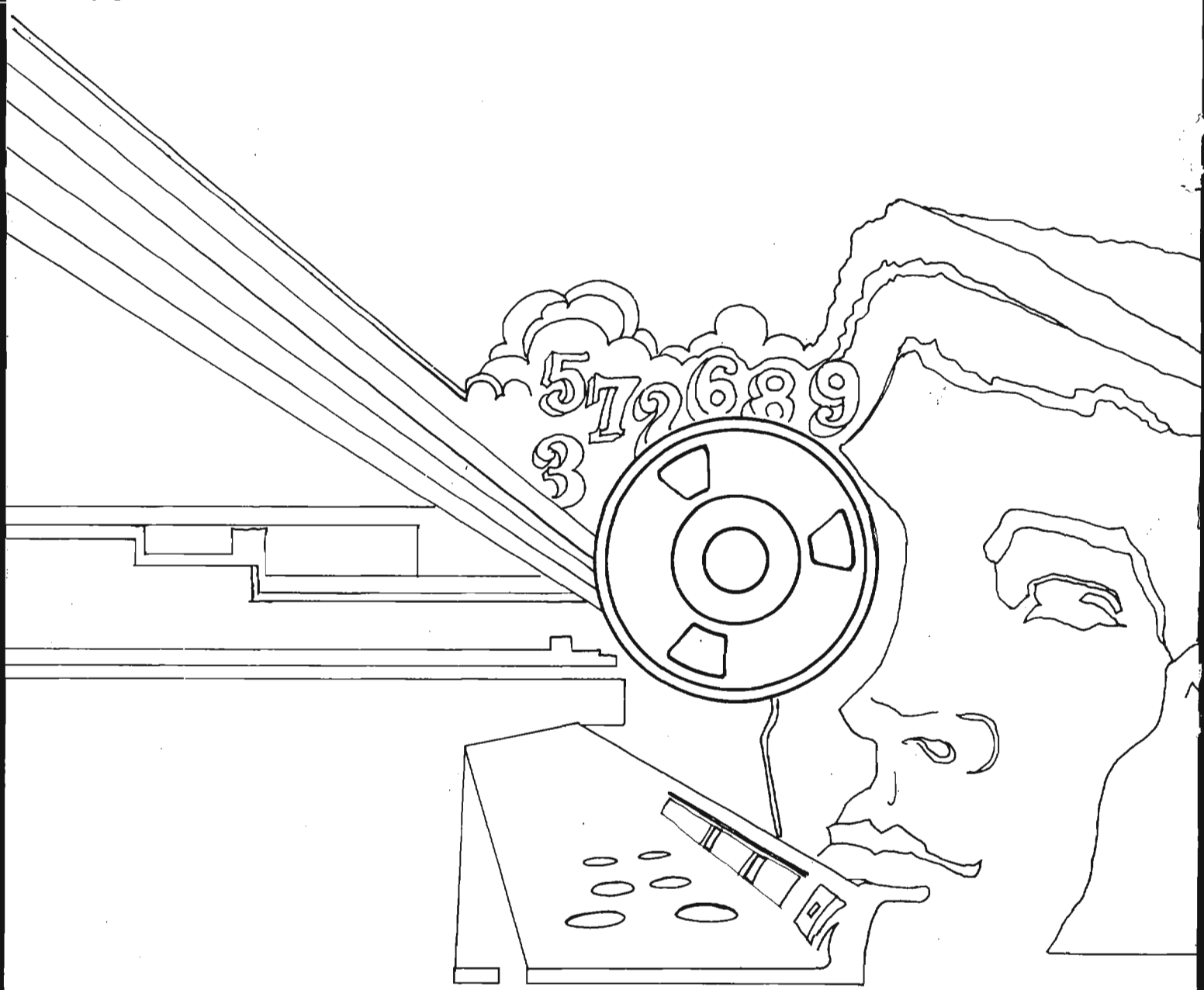
252 220 36 16 157 198 246 93 193 8 108 115

126 165 196

221 120 74 38

11 51 134 13 44 175 249

1 R	2 I	3 O	4 B	■	5 U	6 H	7 J	■	8 Y	9 C	10 R	11 Z_1	12 B	13 Z_1	14 E
15 Q	■	16 Y	17 N	18 W	■	19 O	■	20 M	21 I	22 N	23 E	24 B	25 J	■	26 I
27 R	■	28 Y	29 C	30 N	31 U	■	32 V	33 C	34 O	35 X	■	36 Y	37 L	38 T	39 X
■	40 U	41 S	42 Q	43 Y	■	44 Z_1	45 Q	46 T	■	47 O	48 V	49 U	50 R	■	51 Z_1
52 E	53 Q	54 B	55 S	56 D	■	57 R	58 V	59 Y	60 B	61 N	■	62 A	63 H	■	64 V
65 I	66 M	■	67 L	68 I	69 P	70 Q	71 S	■	72 T	73 J	■	74 Z	75 N	76 B	77 J
■	78 Q	79 B	80 S	81 N	■	82 Y	83 S	84 D	85 T	■	86 A	87 L	88 B	89 G	■
90 Y	■	91 H	92 B	93 Y	94 E	95 D	96 Q	97 I	98 M	■	99 W	100 D	101 V	■	102 Y
■	103 U	104 O	105 E	106 B	107 H	■	108 Y	109 L	■	110 S	111 E	112 G	113 B	114 Q	115 Y
116 S	117 L	■	118 N	119 B	120 Z	121 M	122 U	123 E	■	124 W	125 T	126 Y	■	127 D	128 H
■	129 U	130 C	131 E	132 B	133 N	134 Z_1	■	135 G	136 K	137 J	■	138 M	139 Y	140 M	141 Q
142 C	143 B	■	144 L	145 C	146 B	147 Q	148 E	149 K	■	150 X	151 M	152 E	153 S	154 F	155 B
156 T	157 Y	158 C	159 Q	160 N	161 Y	■	162 Q	163 B	164 H	165 Y	166 O	167 N	168 P	■	169 T
170 P	171 K	■	172 Y	173 E	174 V	175 Z_1	176 B	177 N	■	178 D	179 P	180 C	■	181 Y	182 I
183 R	184 G	185 Y	■	186 H	187 U	188 R	189 A	■	190 K	191 A	192 W	193 Y	■	194 M	195 W
196 Y	197 V	■	198 Y	199 B	200 P	201 E	202 D	203 M	■	204 V	205 W	206 P	■	207 X	208 N
209 A	■	210 J	211 Q	212 S	213 L	■	214 K	215 A	216 U	217 M	■	218 V	219 A	220 Y	221 Z_1
■	222 K	223 H	224 I	■	225 F	226 E	227 F	228 C	229 T	■	230 F	231 R	232 J	■	233 Y
■	234 W	235 G	236 M	237 E	238 J	239 B	■	240 C	241 J	242 Y	243 U	■	244 Q	245 E	246 Y
247 E	248 C	249 Z_1	250 B	■	251 N	252 Y	253 F	254 M	■						D.H.W


5 7 9 6 8 9
3