Declassified and Approved for Release by NSA on 10-16-2012 pursuant to E.O. 13526, MDR Case # 54778

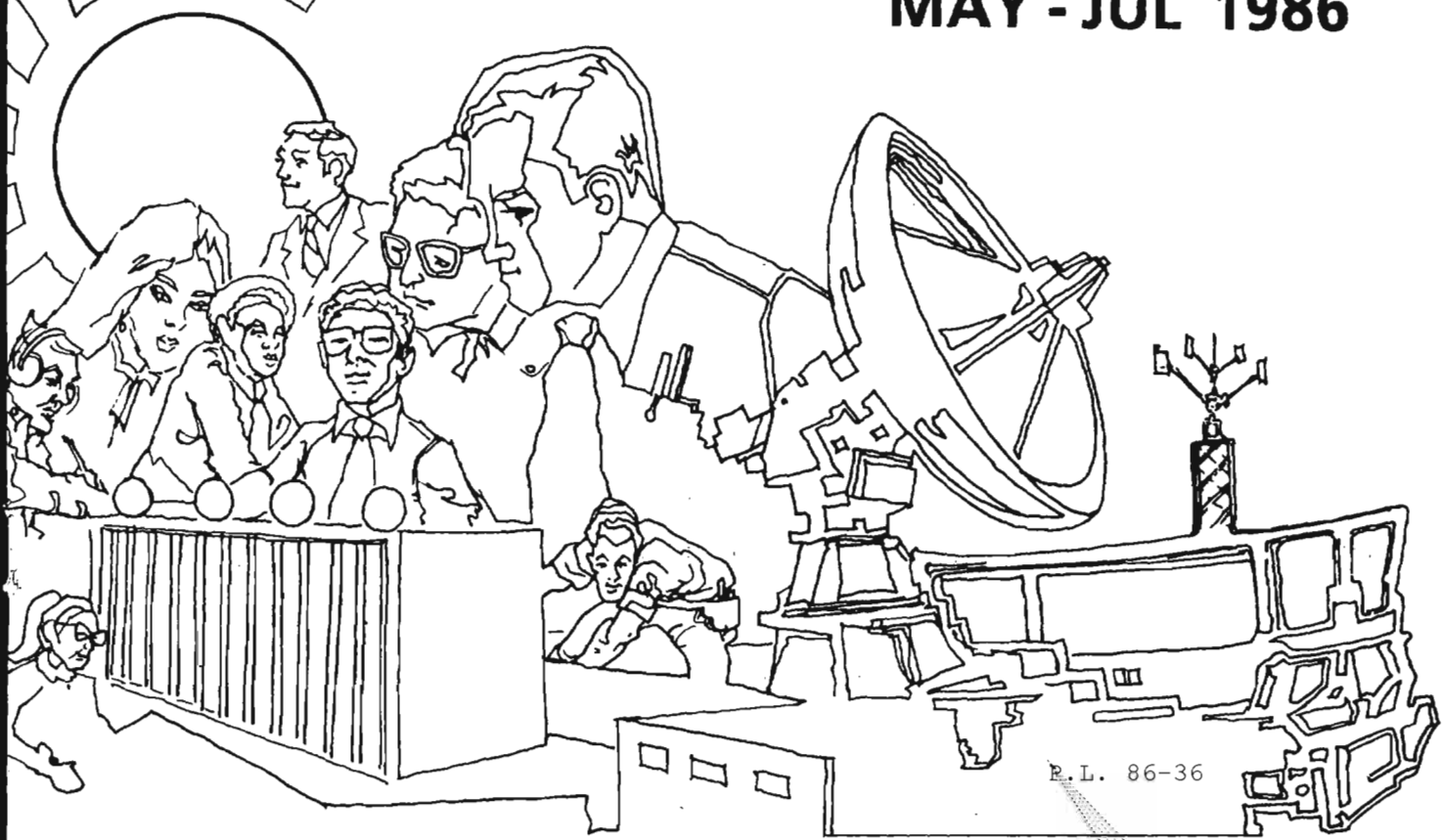
DOCID: 4019705

~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

MAY - JUL 1986



P.L. 86-36

ODYSSEY (U) . . . . . [redacted] 1
BULLETIN BOARD (U) 6
ORGANIZING FOR EFFECTIVE C3 ANALYSIS (U) . . . [redacted] . . 7
A LINGUIST MEETS THE ASTW (U). . . . . [redacted] . . .10
AI AT NSA (U). . . . . [redacted] . . .12
PRESERVING VALUABLE NSA/CSS PAPER RECORDS (U). [redacted] . . .14
TEAM BUILDING (U). . . . . [redacted] . . .18
USER-FRIENDLY PASSWORDS (U). . . . . [redacted] .22
ERRATUM (U). 25
LETTERS (U). 26
OUT OF MY DEPTH #4 (U) . . . . . WES 28
READERS' SURVEY.(U). 29

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

~~NOT Rreleasable TO CONTRACTORS~~

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

DOCID: 4019705

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XIII, Nos. 5-7 ..... May-July 1986

PUBLISHER .....

BOARD OF EDITORS

Editor ..... (963-1103)

Collection ..... (963-5877)
Computer Security ..... (968-8141)
Computer Systems ..... (963-1103)
Cryptanalysis ..... (963-6424)
Cryptolinguistics ..... (963-1596)
Index ..... (963-5292)
Information Science ..... (963-1145)
Intelligence Research ..... (963-3095)
Language ..... (963-3057)
Mathematics ..... (963-5566)
Puzzles ..... (963-6430)
Science and Technology ..... (963-4191)
Special Research ..... Vera R. Filby (968-8014)
Traffic Analysis ..... Robert J. Hanyok (963-5734)

Illustrators ..... (963-3057)
..... (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:
cryptolg at bar1c05
(bar-one-c-zero-five)
(note: no 'o' in 'log')

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

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

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.

P.L. 86-36

ΚΥΔΟΣ

Accolades to the anonymous author at the National Cryptologic School who composed that most absorbing and inspiring tome On Watch. We were privileged to see an advance copy of this classified history.

The purpose, as stated in the Preface, was to "make new employees aware of the unique history of NSA ..." It's doing more than that. It's also informing some of us who played a part in the events described. All too often the participants behind the scenes do not get to see the big picture.

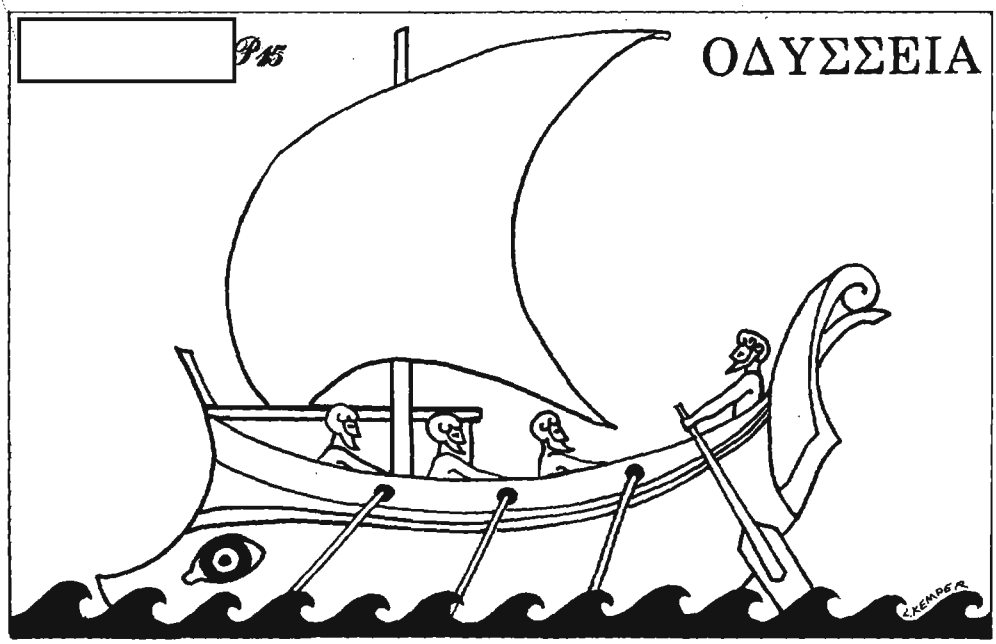
We want more! Don't stop now!

Author! Author!

~~FOR OFFICIAL USE ONLY~~

OCID: 4019705

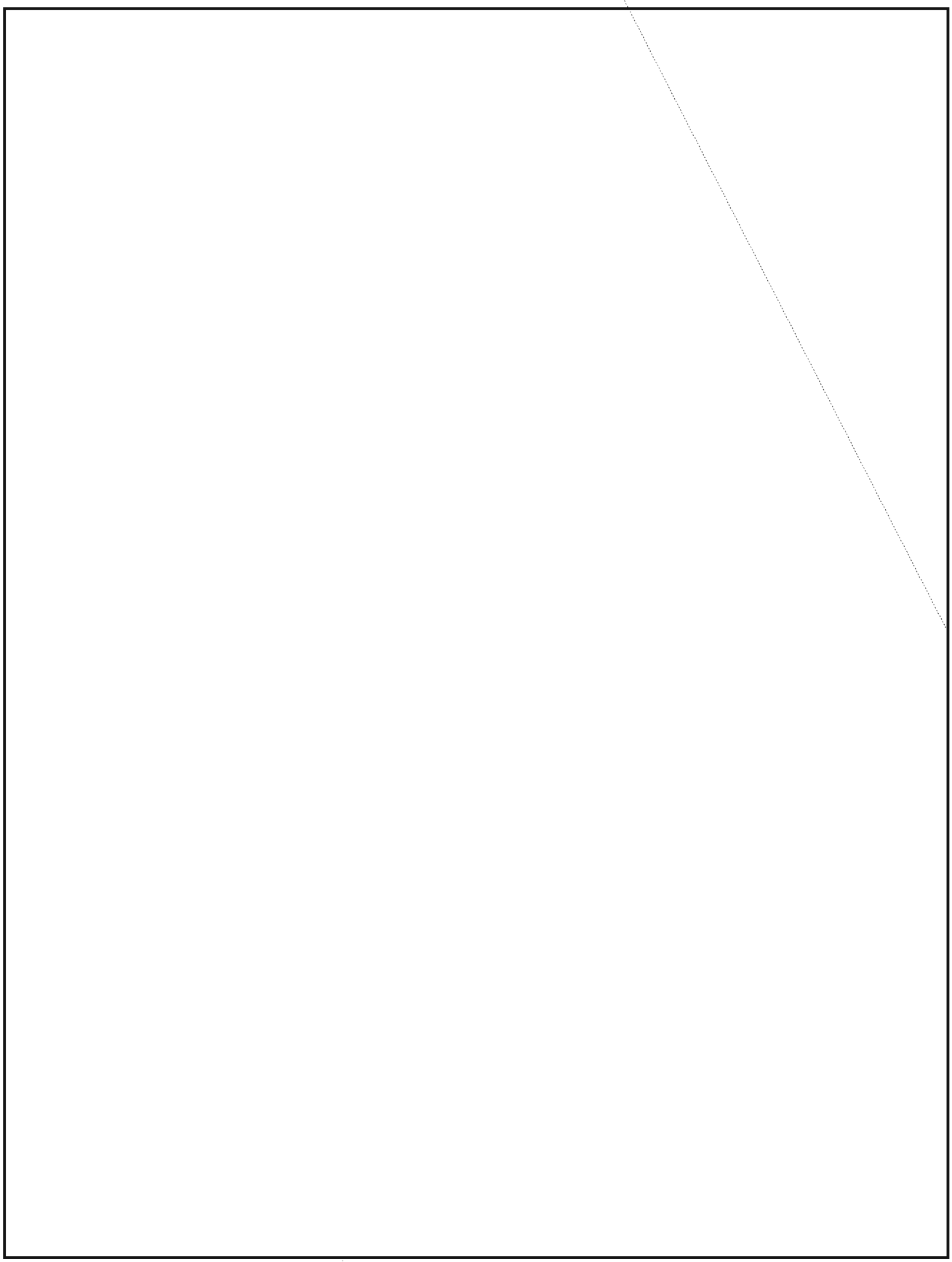
P.L. 86-36



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

DOCID: 4019705

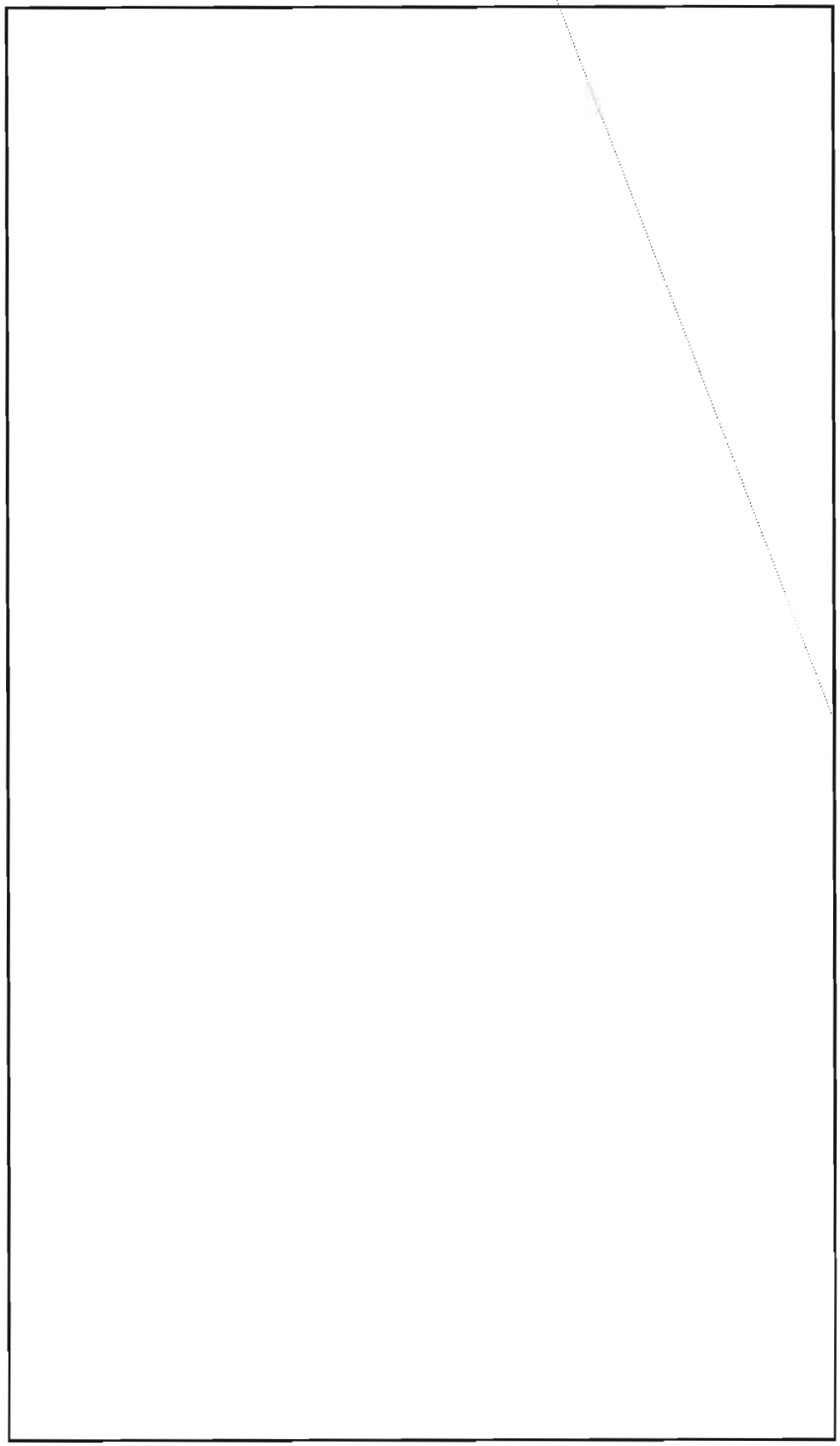
P.L. 86-36
EO 1.4.(c)



OCID: 4019705

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

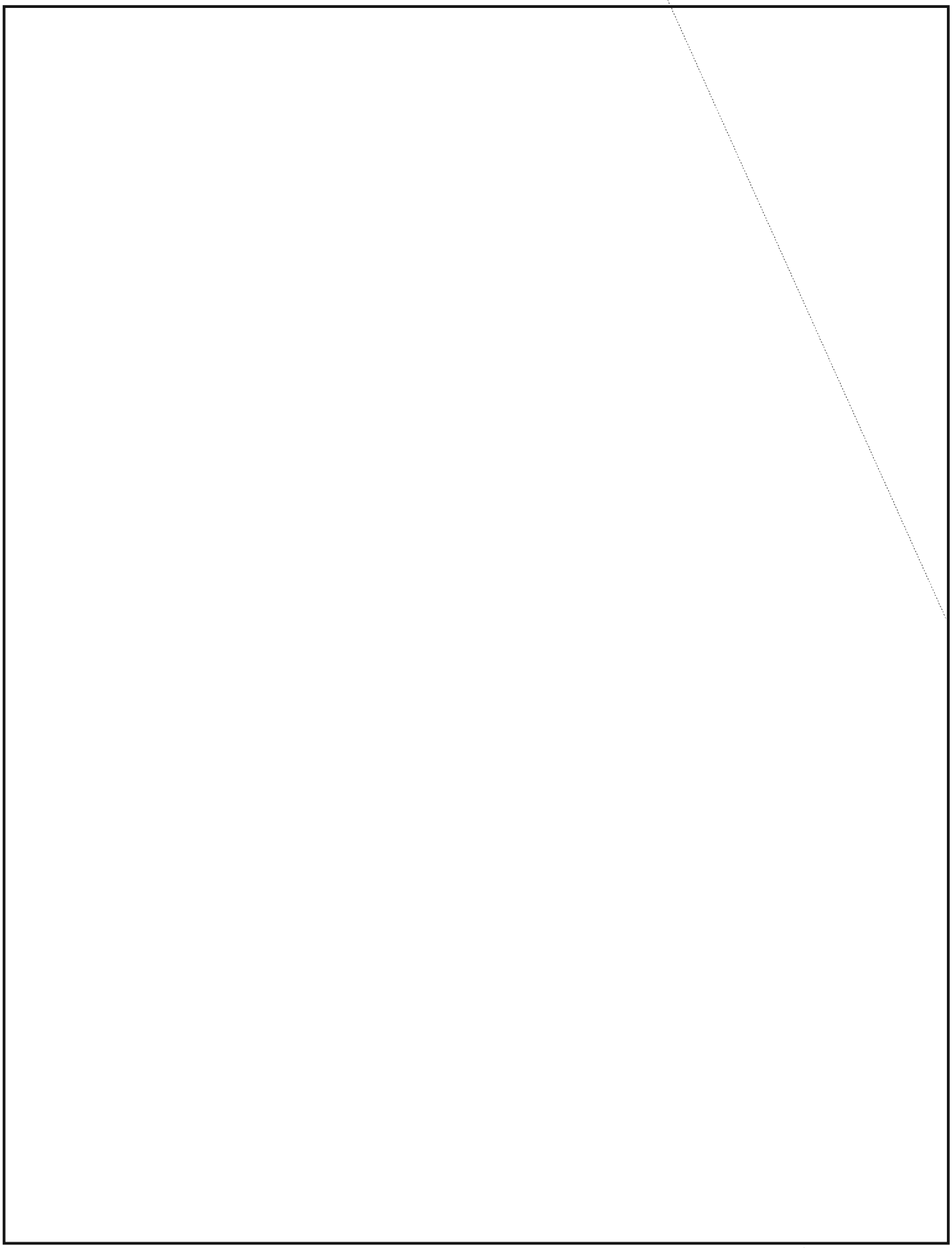
~~SECRET~~



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

DOCID: 4019705

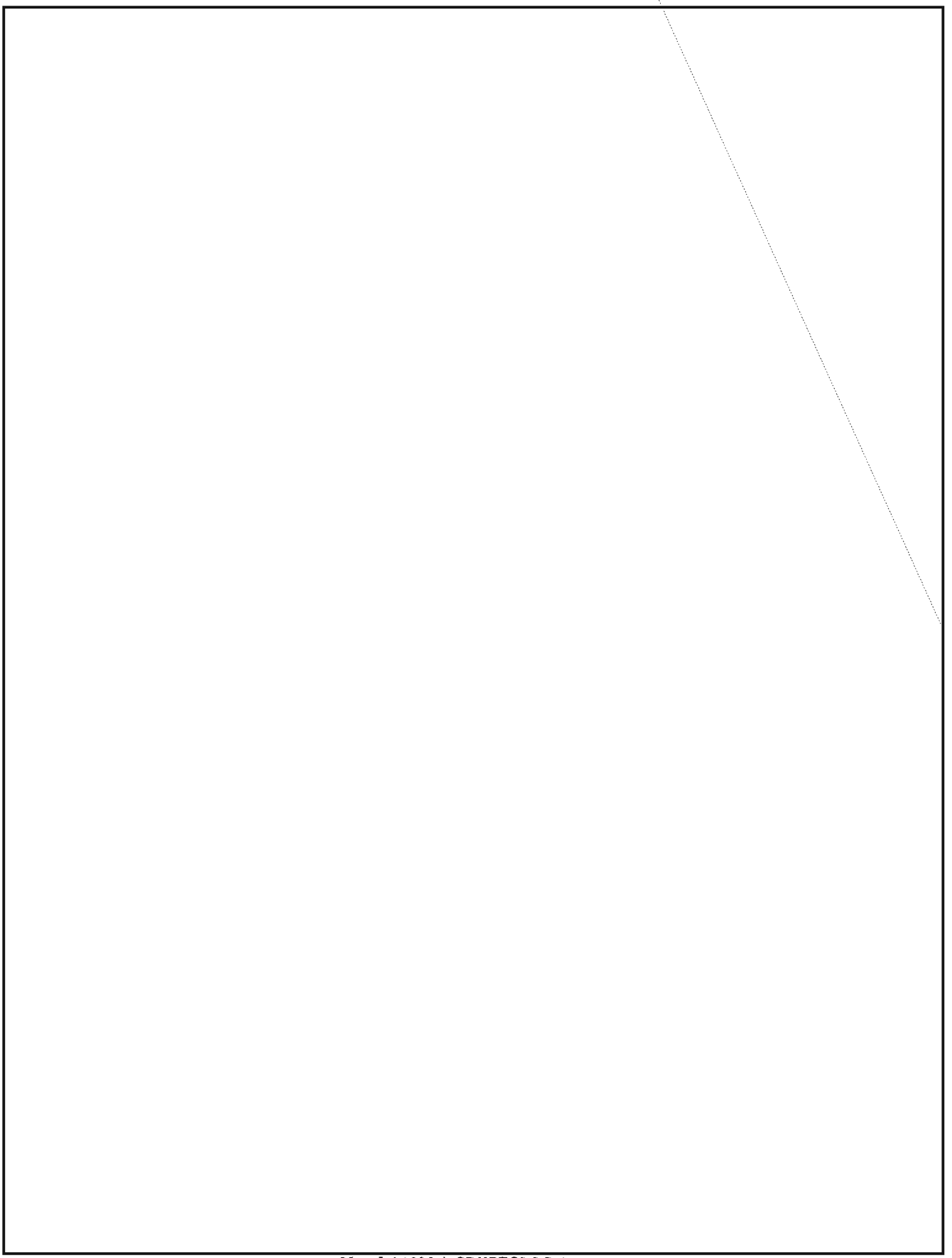
P.L. 86-36
EO 1.4.(c)



DOCID: 4019705

E.O. 1.4.(c)

~~SECRET~~



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

DOCID: 4019705

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

~~SECRET~~

The FOX *and the* CROW.

Answers to:

MORAL DISQUISITION

(Mar-Apr 1986)

Find the five-letter anagram to fill all blanks

"**Spera** in Deo," so the saying goes

(One cannot **parse** it, though the sense one knows.)

However, after "mon **repas**" one day,

When **pears** and port had both been cleared away,

I fell to musing, would God **spare** a Cain

Who **reaps** the heads of men, instead of grain?

At jousts the knight with **spear** to win a prize

Pares his opponents down to half their size

With him is damned the conqueror

To murder, also he who **rapes** and burns.

Answers provided by [redacted] *P16*

BULLETIN BOARD

SPECIAL FOR LINGUISTS (U)

~~(FOUO)~~ Copies of *Collected Articles on Translation, 1973*, are available again. The book, which is classified TSC, contains reprints of articles pertaining to COMINT translation that first appeared in *QRL, Keyword*, the *Cryptologic SPECTRUM*, and *The NSA Technical Journal.*

~~(FOUO)~~ To obtain a copy send your name, organizational designator, building, and room number to [redacted] P16, HQ, 8A187. Telephone orders are not accepted. □

P.L. 86-36

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

OCID: 4019705

ORGANIZING FOR EFFECTIVE C3 ANALYSIS (U)

[redacted]

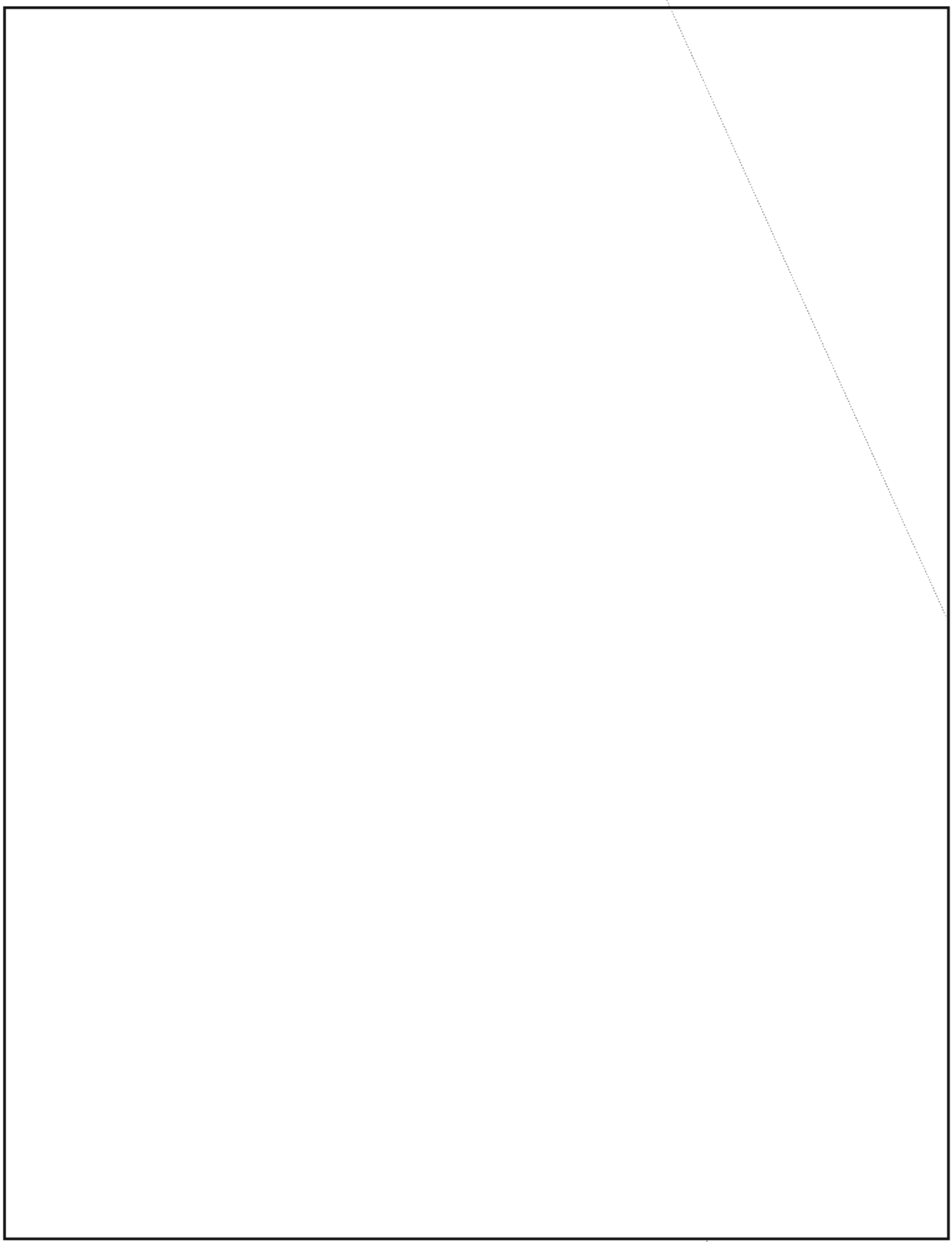
P.L. 86-36

[redacted]

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

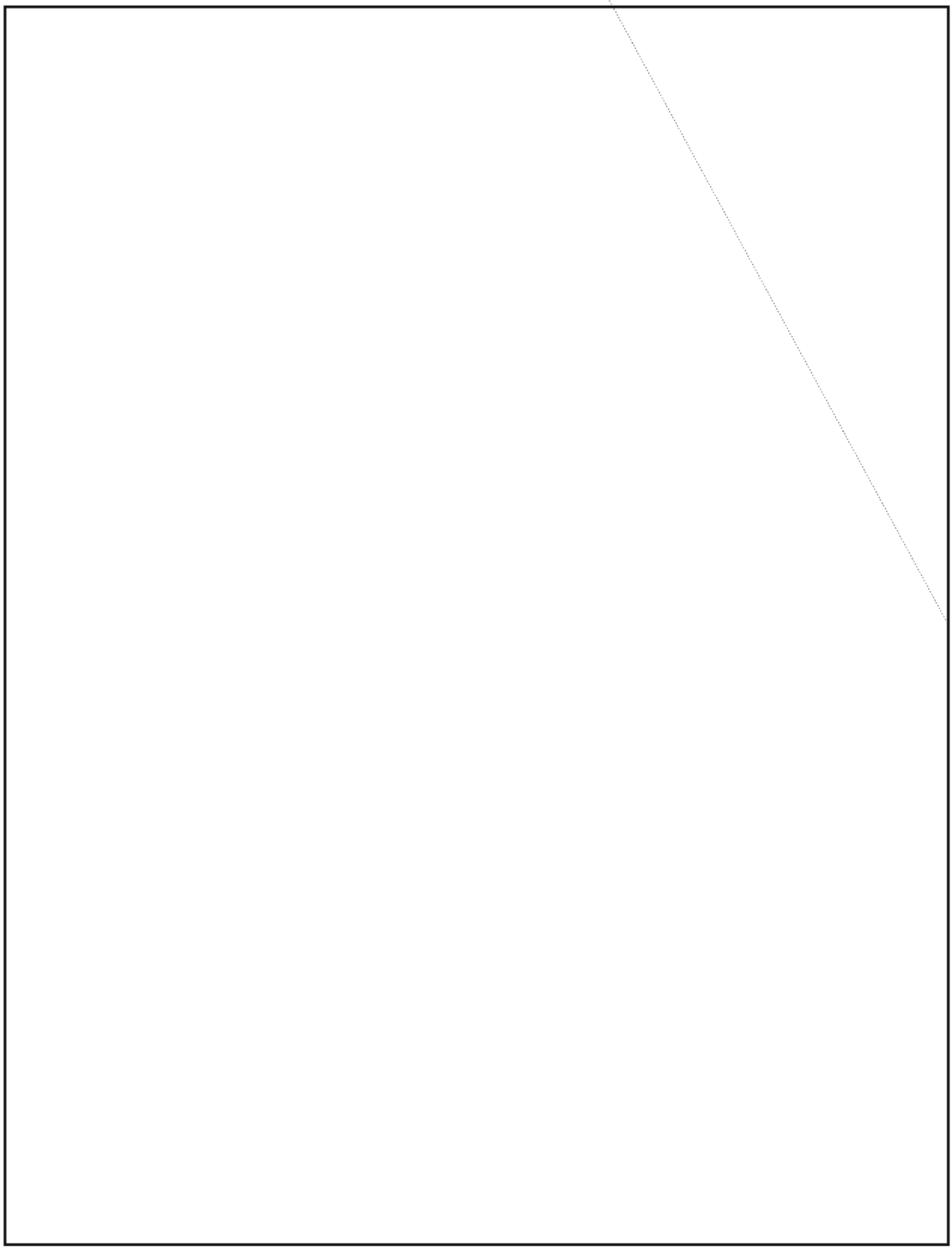
P.L. 86-36
EO 1.4.(c)

DOCID: 4019705



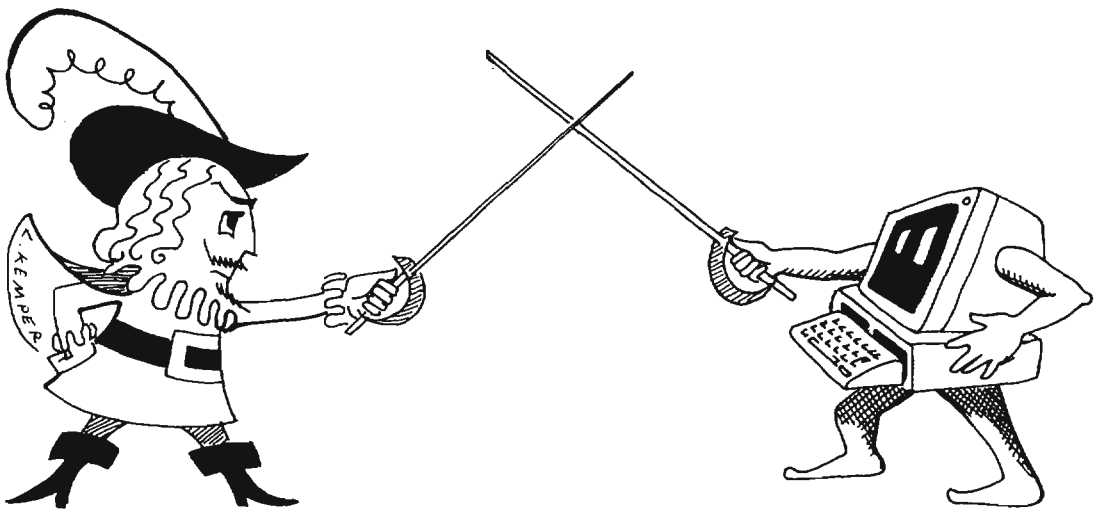
P.L. 86-36
EO 1.4.(c)

DOCID: 4019705



DOCID: 4019705

A LINGUIST MEETS THE ASTW (u)



[redacted] A/SLAG P.L. 86-36

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

Author's Note: The comments below are based on using the UNIX operating system on the ASTW (an IBM XT) and the IBM Graphics printer.

Editor's Note: Readers might be amused to follow the transmogrification of four segments of text as the article flowed from the ASTW monitor to the Star printout, via an IBM floppy converted to an 860 floppy then to an 8010 floppy, and finally output on the Star laser printer. In the text below the segments are shown as converted to the Star. Mel's efforts appear in the footnotes; the first line is the text as output single-spaced on his IBM Graphics printer, and the second line as output on the same printer but double-spaced.

My computer was delivered in a huge box. Surely was glad that my offer to carry it up to my office myself was not accepted. I would never have made it. I unpacked the huge box and discovered a big carton of intimidatingly thick manuals to go along with the computer. Of course, no guidance could I see on how to get started or even on what manual to look in first. Fortunately, in glancing through some of the manuals, I looked in one labled Tu'taProcussi gaGuidu ® and saw that a tutorial was provided. Reasoning that no matter what sort of files I wanted to construct, I would need some word processing functions afforded by the PC/IX operating system, I set about putting myself through the tutorial.

I had been working with the computer 15-20 minutes when I wanted to cancel a command, which is done by pressing the <Alt> and <Lang> keys simultaneously (nothing about "cancel" there - but, really, that's the way it's supposed to be done). Well - clumsy me - my thumb missed the <Alt> key - meaning that I had pressed the unaltered <Lang> key. To my horror, the whole screen was immediately flooded with Cyrillic, the alphabet used for Russian. It wasn't the Russian language, mind you: just the Russian alphabet. I spent about an hour trying unsuccessfully to get out of that - trying to get back the English that I had typed in. Finally, a colleague said that I should press <Ctrl> and <Lang> simultaneously. I tried that - and sure enough I was out of the Cyrillic mode! But when I

tried to type the letter "e" to edit or to create a file, all I got was an "a" with an umlaut (two dots) over it. I struggled with that one about 15 minutes before I somehow got back to "normal" operations.

It turns out that there is a little system file that allows one to set the computer for color (which I don't have) or graphics (which, it turns out, I do have) instead of the monochrome monitor that the computer comes set for. Setting that file correctly takes care of those Cyrillic letters all over the screen when you don't want them there. Anyway, now that I've made the adjustment to the file, I am able to type in Russian when I want to and in English when I prefer to do that.

The only trouble in using Cyrillic is that I cannot sort in Cyrillic alphabetic order and cannot print Cyrillic on my printer. And I have destroyed huge parts of files when I have tried to use some of the normal word processing functions. When I tried to replace a Russian word with another Russian word (quite a normal function for English), all hell broke loose: all but a few words at the left-hand side of my screen were wiped out. That was true throughout the number of lines I had specified for the Cyrillic characters.

Though I can't print Cyrillic, some weird things happen when I try: my printer dances all around, whistles, spews out blank pages, and in general acts like a wild person. Some of the Cyrillic letters have the same ASCII coding as some of the printer control functions. I have harnessed this knowledge to help me in a few instances - e. g., to get a larger print, I just type in the Cyrillic "o", and the rest of that line will print out in double width. Very handy for a major title.

The peculiarities of printing do not end with the Cyrillic story. They extend to English iua ouatr atoau durli u. ③ After hitting <Alt> "f" (for font), the text will appear underlined and in reverse video on the screen. Then, using the print command ($print filename), the nice underlined portion in English shows up on the printed page as European letters with diacritics and graphics characters!

Within a few days after getting into operations, I really did it to myself again - or maybe the system did it to me. Curious about what the "Menu" under Function Key 1 (F1) was, I pressed that key. Three options appeared on my screen. The third one was "Edit your editor profile." Naturally, I wondered what my editor profile was, so I chose that option. But only a blank screen for creating a file came up. The only way to get out of that was to press <Alt> "d", which "copies" a file. But then when I tried to create new files or view old ones, I could not invoke the editor - that is, I could not do a blasted thing. It turned out that the editor profile (.eprofile) file overrides the normal system commands for the editor and that a blank file (which I had just created) means to do nothing. And the computer was doing exactly what I unknowingly had told it to do - otui g. ④ The solution to the problem was to delete the .eprofile file.

At first, I spent a great deal of time trying to figure out what all the keys on the keyboard meant when I pressed the <Alt> and a given key. But finally I found a little picture of the keyboard in the manual cited above, the Tu'taProcussi gaGuidu ⑤ (p. 2 of the "INed" section). I cut the picture out and pasted it on my keyboard, and that made life a lot easier for me. I had to be sure to change the position of the CAPS LOCK, CTL, and ALT keys in the picture to fit the reality of my keyboard.

The ASTW using the PC/IX is, indeed a powerful and flexible device - one that is sometimes quite a pleasure to use. But frustrations that anyone might well suffer are compounded for the linguist when he tries to make his machine truly bilingual.

① ∟σ° ⌠á⊥≥∩πσ≤≤θ∈τá⌡ θΣσ
Text Processing Guide

② θμá·∩⌡á⌠≥·á⌠∩á⌡∈Σσ≥ωθ∈σ.
if you try to underline.

③ ∈∩⌠δθ∈τ.
nothing.

④ ∟σ° ⌠á⊥≥∩πσ≤≤θ∈τá⌡ θΣσ
Text Processing Guide

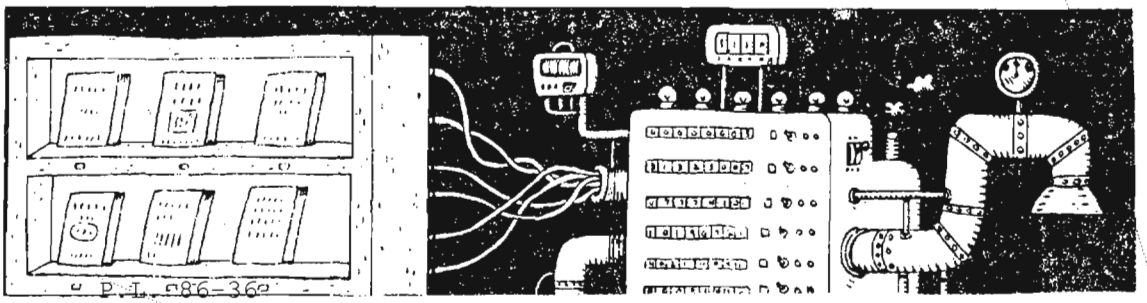
←——————————→

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

P.L. 86-36

AI AT NSA (U)



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

(U) Approximately two years ago the NSA Artificial Intelligence Working Group was formed to introduce AI to Agency tasks, with emphasis upon identifying suitable projects, and to establish a forum for the orderly exchange of information among Agency personnel and with outside sources. The Group, chaired by Norman Glick of Z, comprises representatives from many Agency elements in which AI techniques are being studied and applied, thereby avoiding duplication of effort.

(U) Development of AI at NSA began with the procurement of hardware and with the training of personnel. The Pentagon agency DARPA (Defense Advanced Research Projects Agency) provided NSA with several Symbolics 3600s, computers designed specifically for AI applications. The 3600s are now placed in offices throughout the Agency. Training is available both outside and in-house. Johns Hopkins Applied Physics Lab has a Master's degree program in AI and George Washington University a program in knowledge engineering, a skill essential to the construction of an expert system. NSA offers a self-paced video course in the Learning Centers and a platform course on LISP, the AI programming language most popular in the United States. A three-day Technical Development Program Seminar entitled "Overview of Artificial Intelligence Research and Applications" was held in January, 1986. Agency personnel have participated in conferences and seminars on AI, some of which have been hosted by NSA. The NSA libraries contain many books on AI, ranging from introductory surveys to highly technical material.

AI PROJECTS AT NSA

~~(C-CCO)~~ Information about AI projects at NSA was obtained through interviews with individuals who are applying AI techniques to Agency problems. Following is a small sampling of applications in progress at NSA.

W1

(U) (American industry is currently using a similar process, in which "seeing" robots compare product parts against a model to search for anomalies that could indicate a faulty product.)

(U) The development of W1's expert system was shared between NSA personnel and a contractor. W1 supplied two experts for the initial stages; when the contractor eventually took over, he was able to provide analysts with related expertise. The interaction between the experts and the knowledge engineers (those responsible for collecting the expert's knowledge and organizing it into machine-comprehensible form) took no fewer than five rounds. This project was concluded just in time before the two W1 experts, upon whose knowledge this system was based, left the project.

~~(S)~~ W1 already has one Symbolics 3600 computer and is expecting two more, along with additional hardware such as an experimental workstation. The new equipment will be compatible with other hardware used by W1, including VAX, IBM, and CDC computers. As each stage of the AI system is completed, it is implemented in that operational element, thereby allowing the analysts to give feedback during the development stage. Implementation of the expert system could reduce the time spent in analyzing one event from several months to less than a week.

G424

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

~~(FOUO)~~ [redacted] a graduate of the CA intern program, is trying to develop an expert system to avoid such a situation. Along with [redacted] of G431, she was awarded a grant for this project from the NSA Director's Skunkworks Fund, an account designed to support innovative approaches to aspects of the Agency's mission.

~~(TSC)~~ Development began with selecting a commercially available expert system shell. Using an existing shell saves development time; moreover, eliminating the need to create a shell allows the development team to be composed entirely of cryptanalysts, without external computer programming support. The selected hardware, a Symbolics 3670, has already been installed. Upon receipt of the software, formulation, testing, and modification of the expert system can take place.

AI AS A POSSIBLE CA INTERN TOUR

~~(C-CCO)~~ [redacted] found that, even as a permanently assigned cryptanalyst, it took him nearly three months to acquire sufficient background to be useful to the A54 expert system development team. [redacted] on the other hand, believes that an intern can play a useful role in certain stages of the development of the G424 expert system.

~~(C-CCO)~~ It may be of interest to note that neither of the intern graduates (Susan and Steve) had courses in programming or mathematics before coming to the Agency; since then Susan has taken courses in programming and math, and Steve in programming Susan suggests the following as minimum requirements for an intern who might be interested in her AI project: basic knowledge of NSA data systems, familiarity with the rudiments of CA, and successful completion of the probability/statistics course(s).

ACKNOWDGEMENTS

(U) I am grateful to [redacted] for their considerable assistance and to [redacted] for classification review. □

CID: 4019705

PRESERVING VALUABLE NSA/CSS PAPER RECORDS

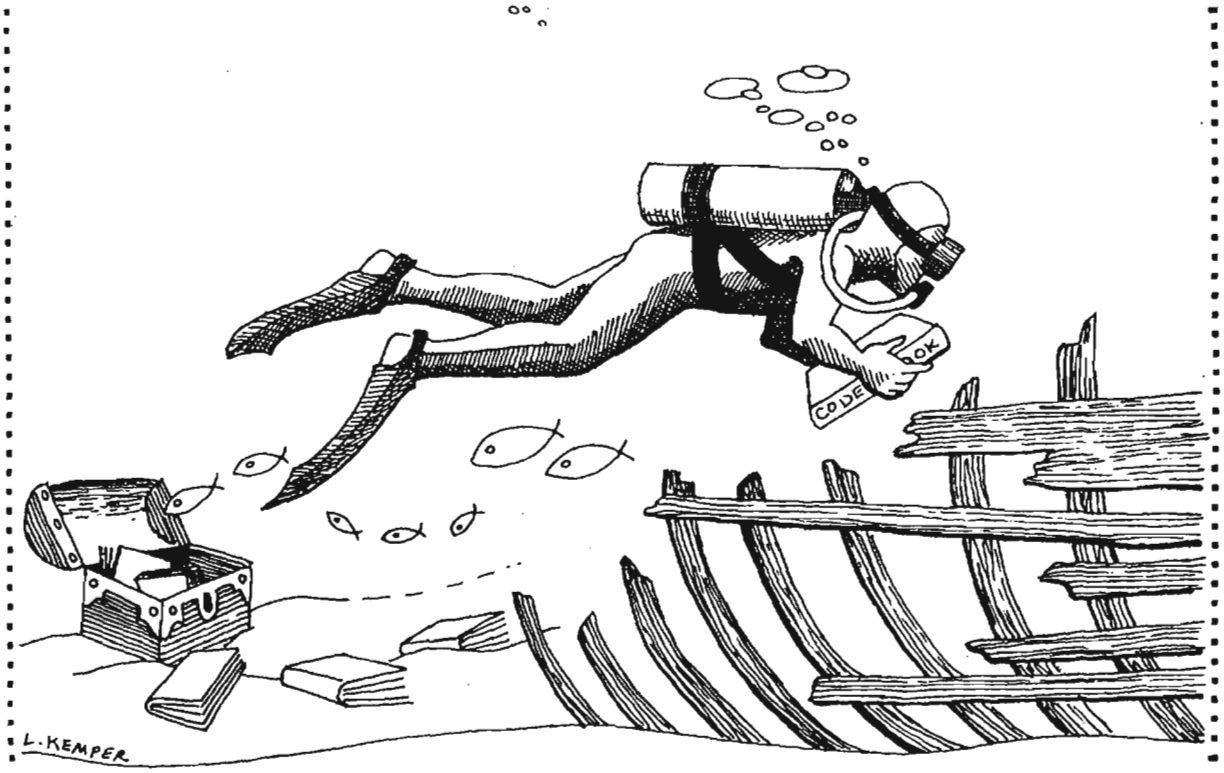
[redacted] T54

P.L. 86-36

Most paper records are valuable only for the information they contain and, therefore, the medium in which the information is held is normally irrelevant. In such cases, it suffices that the information be portrayed as a true copy and be easily accessible and readable. Beyond this, there are some paper records that have intrinsic value. In such cases, ways must be found to preserve the original paper medium from the deleterious effects of rough use and poor storage conditions, or to conserve it by appropriate restoration techniques when damaged.

In recent years, NSA/CSS has become a leader among Federal Government agencies other than the National Archives and Records Administration (NARA) in the effort to preserve valuable paper records. "Normal" Federal agencies usually transfer their inactive permanent records to NARA control long before they are so old that a critical stage is reached in their physical existence. However, almost all of our records still require restricted access and special security handling, even after they become fully inactive

For this reason, they are not stored with the records of other agencies at a Federal regional



~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

records center, or at the National Archives building itself. Because of this, NARA has given NSA/CSS special permission to retain its classified permanent inactive records in a special Cryptologic Archival Holding Area (CAHA) until they are fully declassified and can be released. [As an aside, there are perhaps only two or three archival holding areas permitted in the entire Government.]

Recognizing that declassification may be many years away for our permanent records, NARA has also required, and NSA/CSS has agreed, that we undertake special measures to preserve them. What follows is a description of the system that the CAHA staff has devised to carry out this task.

But first, some background information on preservation techniques is necessary. Preservation includes passive measures taken to insulate or protect records from external forces or influences that attack, make unreadable, or eventually destroy them. This includes inhibiting the transference of acid between the pages of paper articles, and the boxes, folders, or containers housing them; isolating paper from exposure to ultraviolet rays emitted by the sun or fluorescent lighting; removing rustible bindings; and, protecting paper from adverse environmental factors such as excessive heat, humidity, flooding, and pollution -- all of which embrittle, fade, debilitate or otherwise destroy the cellulosic fibers of which paper is composed. Preservation also includes taking appropriate active conservation methods, to include those that directly affect or change the inherent structure, properties, or composition of paper. Included in this are deacidification-encapsulation, mending, and restoration.

Active records in NSA/CSS "mature" and reach a final disposition stage at varying periods, as described in our four Records Disposition Schedules (RDS). The RDS's are titled: Signals Intelligence, Communications Security, Research and Evaluation, and Administration-Management. At some point, the records in these schedules become candidates for either destruction or permanent preservation. The RDS's are approved by the Archivist of the United States, who is the final authority on whether a given record is permanent or temporary.

In NSA/CSS, when a permanent record reaches its 20th - 30th year, it is ready for processing into the CAHA. It is at this juncture that CAHA archivists begin to apply preventive maintenance preservation measures. Staples, clips, rubber bands, metal fasteners, and all similar binding materials that rust and adversely interact with paper are removed; folders and containers laden with acid are replaced by acid-free ones. Other minor repairs to damaged paper records are made at this time.

While gathering and inputting information designed to give us good intellectual controls over records in a storage area, as well as the usual bibliographic controls needed, agency archivists also identify records that require advanced preservation treatment. This includes cleaning, flattening, deacidification, encapsulation, etc. The Archival Information and Retrieval System, an automated finding aid system in use in the CAHA, is then annotated as to what further preservation measures are needed. When the required controls have been established, review for continuance of classification has been made, and all finding-aid data have been entered into the system, records requiring advanced treatment are queued until an archivist-conservator has the time to process them further.

In NSA/CSS, active preservation for valuable permanent records includes state-of-the-art as well as centuries-old archival conservation techniques. CAHA archivists dry-clean dirty documents with opaline and other compounds and repair ripped or torn pages with long-fibered Japanese papers appropriately matched for color and texture, and home-brewed wheat starch or methyl cellulose pastes. Paper can be deacidified with non-aqueous chemicals that also leave a protective coating of alkaline on the paper's surface. To further protect documents that have become so embrittled, spotted, or worn that more handling might jeopardize them, archivists encapsulate. Encapsulation is the enclosing of a document (preferably first deacidified) between two sheets of an acid-free, ultraviolet ray inhibiting polyester material. The two outer polyester sheets create a field of static electricity (after vigorous rubbing with a clean cotton pad) that effectively grips the sandwiched sheet of paper and permits its safe (even *rough)* handling. The polyester keeps out dirt and other airborne pollutants and its U/V shield repels the fluorescent light/sunlight rays that attack exposed paper.

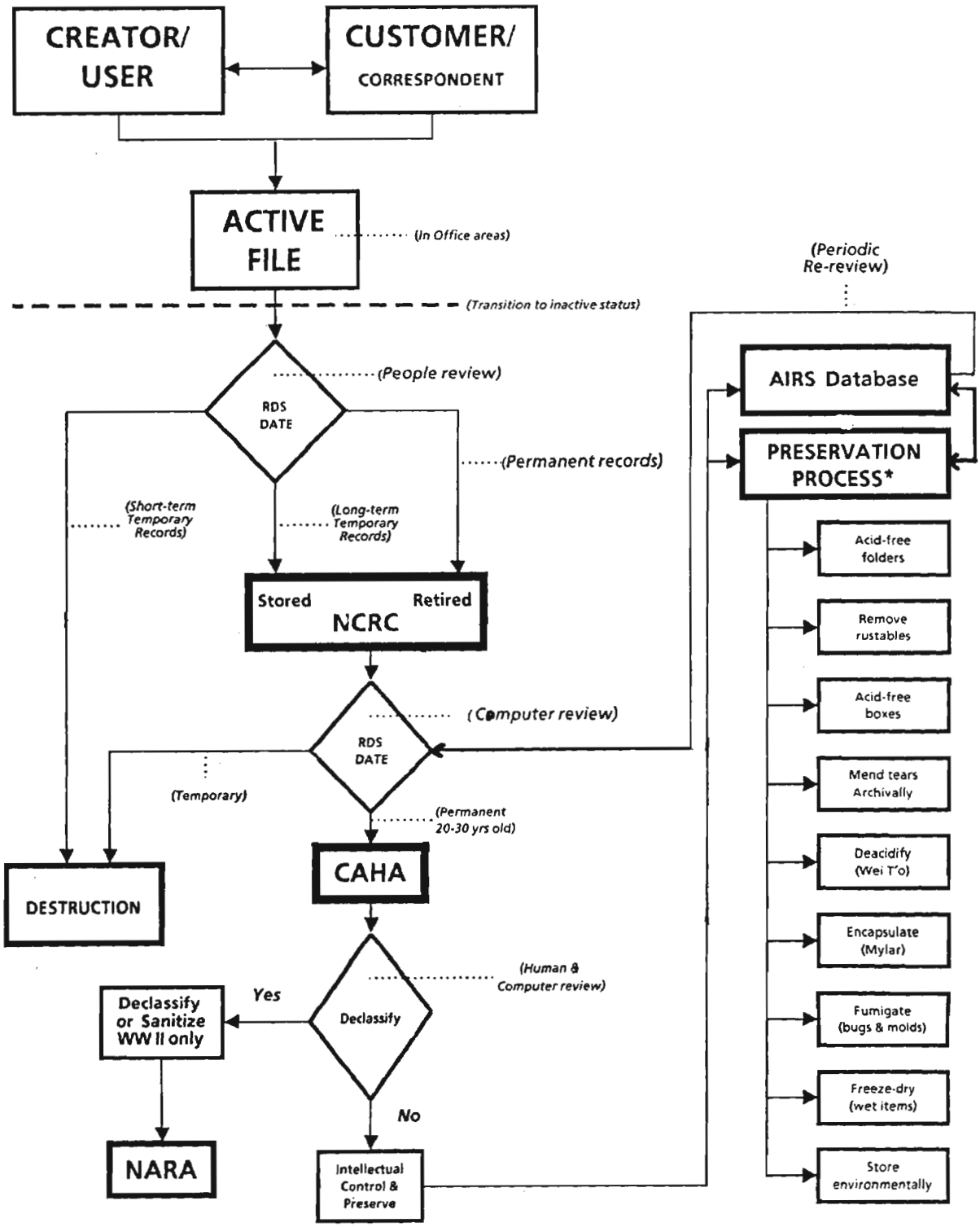
Best of all, encapsulation is fully reversible and one need only rip open the electrostatically sealed (special machine-generated) seams, none of which have touched the paper, to get back to the document in its original state.

The CAHA's latest preservation acquisition is a freeze drying chamber capable of holding and treating up to 16 cubic feet of records. It provides our most exotic preservation capability. Imagine having a very valuable operations-related document fished out of a cesspool after

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

THE NSA/CSS PERMANENT DOCUMENT PRESERVATION CYCLE



* As needed and authorized by the NSA/CSS Archivist

Abbreviations Key

RDS	=	NSA/CSS Records Disposition Schedules (4)
NCRC	=	NSA/CSS Records Center
CAHA	=	Cryptologic Archival Holding Area
NARA	=	National Archives and Records Administration
AIRS	=	Archival Information and Retrieval System

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

abandonment by a target, or recovered from a safe in a sunken vessel. What is the normal state of such a document after it has been subjected to the usual methods of drying? Shriveled, bulged, warped, cockled, or drawn pages, permanently stuck together; totally smeared or obliterated ink or pencil entries; key words and phrases in the text covered by impenetrable stains or accretions. Not a very good document to work with.

With the lyophilization (freeze-dry) process of recovery, a 99% readable and usable document can emerge. First, however, the document must either be kept in its wet state, or be frozen. (If such a document were delivered to the CAHA in a bucket of water, it would first be frozen.) After the freeze drying chamber has been sealed and all the air evacuated to create a vacuum, the process would begin. It essentially involves removal of the ice from the fibers of the paper by conversion to vapor and then reconversion to ice in an accumulator chamber. The amount of ice removed is weighed periodically to determine just how much water has been removed from the paper. When "just enough" water is left, the process is stopped. At this point, a highly readable and usable document emerges.

This process works equally well for recovering electronic equipment that has been inundated. [The CAHA recently offered its facilities to NASA if it needed help to restore electronic parts recovered from the exploded shuttle; our help was declined with thanks because all recovered equipment was impounded by the investigating board.]

There is also a bit of serendipity attached to our acquisition of this device. We have since discovered that it can function very efficiently as a paper fumigator. When paper lice, mites, and other live things are found in old boxes, we can quickly freeze the entire box, killing all the live things, and then create a vacuum, which effectively explodes and destroys any eggs about to hatch.

The agency now has other tools available to make operational tasks easier. If you have an intrinsically valuable document that has been soaked (remember the recent flood in the computer operations area of the Operations building basement?), or if it is infected with lice or is otherwise too fragile for continued use, call the author or the CAHA staff (972-2268s) for assistance. □

Solution to Essex Cipher, War of 1812 (Jan-Mar 1985)

```
.QD66.94DK.C7.G4C66C.
.SELL THEM IN CHILLI.

.AP8QPD2.
.PURSUED.

.A8DAF8D2.
.PREPARED.

.AX6C9CGF6.
.POLITICAL.

.7X9.7F0CBF9D.94D.AFGC3CG.C7.QF3D9O.
.NOT.NAVIGATE.THE PACIFIC.IN.SAFETY.


 Plain:  A B C D E F G H I J K L M
Cipher:  F . G 2 D 3 B 4 C . . 6 K

 Plain:  N O P Q R S T U V W X Y Z
Cipher:  7 X A . 8 Q 9 P 0 . . O .
```

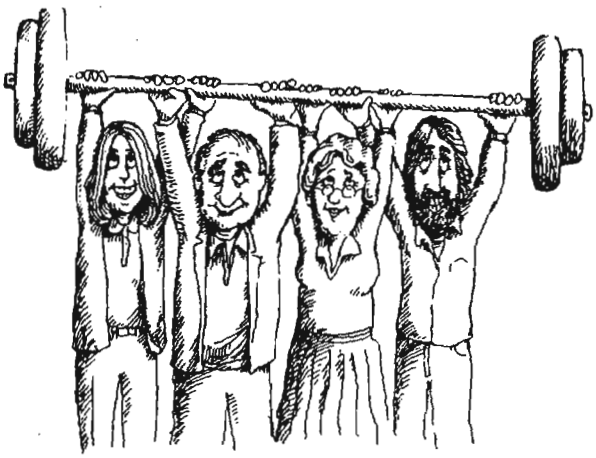
Readers are invited to submit a complete solution of the substitution system.

~~FOR OFFICIAL USE ONLY~~

CID: 4019705

TEAM BUILDING

A TOOL FOR IMPROVING ORGANIZATIONAL EFFECTIVENESS (U)



E622

P.L. 86-36

Imagine the people in your organization--even the most indifferent--suddenly finding new excitement and challenge in the job they now take for granted. What would it be like to have a management team that plays the "What Might We Do" game and not the "Ain't It Awful" game?

All this and more can happen when an organization makes a decision and commitment to work as a team. A formal team building workshop may be all that you need to start improving your organization. Following is an explanation of what team building is and is not, and how it might help your organization become more effective.

Only a very small part of a manager's or executive's work is spent in isolation; most of the time is spent working as part of a team in project meet-ings, committee meetings, executive teams, staff meetings, and task forces, as well as in other "teams" -- family, fraternal, political, recreational, and religious. Yet many managers do not know how to function either as a team member or a team leader. They can learn, however, by participating in team-building workshops.

Team-building workshops are designed to:

(1) enhance the effectiveness of persons who share goals and are dependent on each other for achieving them;

(2) increase collaborative efforts to achieve both individual and team objectives.

During the past 15 years, team building, a facet of organizational development, has emerged as a major technique to improve the way in which work is accomplished by individuals who have common work relationships and goals.

WHAT IS TEAM BUILDING?

Team building is a planned and managed event involving a group of people who have common organizational relationships and/or goals. In the Agency, team-building workshops are conducted primarily to help the organization achieve optimum organizational effectiveness, and are problem-solving oriented, that is, they center around accomplishing tasks. Team building should not be confused with "T-Group" or "sensitivity training" which was popular in the 60's. Sensitivity training focuses primarily on the individual in interpersonal relationships and

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

on the emotions, such as hostility and anger, surrounding the relationships.

The team-building process requires a trained internal (E62) or external (contract) consultant who assists the group members to work through semi-structured or structured activities and work-related problems. The object is to develop and sustain positive, integrated work relationships so that the members function more effectively together. While a workshop may center on the tasks and activities performed by a particular group, it must also focus on the team-action production process. Thus, it tends to be more **process** than **content** oriented.

Occasionally, teams meet to work on specific issues or problems without the aid of a facilitator or consultant. These sessions are generally called management retreats, project meetings, or planning meetings, and tend to be mostly content-oriented.

Quite often a question arises about the need for an external facilitator. We have learned that teams who use a member of their own organization -- a division chief, staff chief, or executive -- as a facilitator for their initial attempt at a team building workshop are less successful than those which are led by a trained facilitator. That may because the team-member facilitator may be a part of the team's problem, or perhaps because a team-member facilitator becomes so involved with the content and with solving content problems that the process goes unattended; thus the purpose of the workshop is defeated. But once team members learn to work together and manage the team process, there is usually no further need for an outside consultant.

TYPES OF TEAM-BUILDING WORKSHOPS

There are several varieties of team-building workshops:

- family team building workshop--a division chief and the branch chiefs;

- start-up team building workshop--members from various organizations can be used as a means of getting a project or organization off to a spirited start;

- transition team building workshop--designed to integrate a new manager such as a field station chief, office chief, division chief, etc., into an existing team. The objective is to minimize disruption of work and to reduce the time it takes a manager to become acquainted with the management team;

- follow-up team building workshops --designed to review progress on action items from a previous team building workshop, identify new issues and concerns, and develop action plans to create the desired change. Follow-up workshops are routinely conducted four to six months after the initial workshop.

All team building efforts are an approach to improving working relationships so as to result in more effective functioning as a group and in accomplishing a task. The key point is that team building is centered around mission accomplishment.

THE PROCESS

To have the greatest impact, team building needs to start at the top of the organization. Starting at the bottom is an exercise in futility since some of the top-level managers might not understand exactly what is taking place. At a minimum, the leader or team must brief upper management on the team's intentions and provide adequate follow-up data on actions the team has taken or expects to take. Also, it must give periodic briefings to inform management of the results accomplished through its efforts.

Individual consultants have their own style of conducting a workshop. After an internal or external consultant is selected by E62 to conduct a workshop, the consultant meets with the manager to discuss the goals of the workshop. Some consultants conduct interviews with every participant, while others conduct interviews with only a few; still others conduct no interviews at all. Some consultants make extensive use of questionnaires before starting, and others collect data during the initial segment of the workshop. Some consultants set an agenda prior to the workshop; others prefer to be flexible and develop it as the workshop progresses . No one method seems to be more effective than the other. The key to success seems to require two things: a consultant who is sufficiently skilled in consulting procedures and team work techniques, and a team which understands the objectives of the team-building session prior to going to the workshop.

At a minimum, the workshop must focus on developing action plans to create some kind of positive change. When teams fail to develop action plans or develop only superficial plans, the workshop has minimum impact on the organization, and in some cases, a negative one.

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

This may happen because though there is awareness of a problem, nothing is done about it.

Following is an example of a team building process commonly used by external and internal consultants conducting Agency workshops:

The team warm-up phase:

◆ identifying factors influencing functioning as a team

◆ creating a team climate for optimum functioning

The team-diagnostic phase:

◆ identifying concerns influencing individual and team performance and satisfaction

◆ collecting data, acquiring data feedback, and planning action

The team-prescriptive phase:

◆ enhancing creative team problem-solving

◆ developing skills for improving individual and team performance

◆ developing mutual coaching skills

◆ learning to analyze team effectiveness

The team action plan phase:

◆ converting options to action items--making it happen

◆ committing resources to optimize team effectiveness

The team implementation phase:

◆ identifying and managing hindering factors

◆ identifying and managing facilitating factors

The team assessment phase:

◆ establishing criteria for team evaluation

◆ identifying means for continuing team improvement

RESULTS

The product of every team-building workshop, in addition to a general feeling of cooperation and trust, is a set of action plans that address areas for improvement. These areas frequently include: how to solve problems, make decisions, formulate policy, set goals, communicate, relate on an interpersonal and organizational level, set stan-dards, and so on. A useful format for action plans is "who, does what, with whom, by what date for what purpose?". A typical action plan might be:

> By 1 January develop a plan for reorg-anizing. George will develop and coordinate the plan with XX and have a proposal for discussion at the next corporate review on 1 November.

The benefit of reorganizing will be less duplication of effort and more equitable distribution of the work load.

While managers have reported a wide span of results, almost all of the feedback indicates that team-building workshop benefited the organization by:

1. Making the team a more effective problem-solving unit.

2. Providing the team a more effective climate in which to work.

3. Developing more openness in communication about issues that are central to the team and the individual effectiveness of team members.

4. Increasing an awareness of and competence in dealing with conflict and change.

5. Developing a new understanding of how the group operates and the benefits of the participative management process.

6. Expanding insights into the members' and the team's roles and purposes in a larger setting.

7. Increasing the team's ability to work with other teams.

8. Developing a stronger feeling of support and interdependence among members with more emphasis on collaboration and less on competition.

In order for a team-building workshop to be successful, several conditions should exist which include:

1. A desire to change;

2. A minimum of severe interpersonal problems.

~~FOR OFFICIAL USE ONLY~~

OCID: 4019705

3. A firm commitment to follow up and evaluate activities and action plans.

4. An adequate amount of time for the session--normally three days -- and subsequent project meetings.

5. A competent consultant/facilitator.

6. A manager or executive who is prepared to deal with a more open and candid system.

7. A manager or executive who is willing to genuinely support the team's desired, legitimate outcome.

LIMITATIONS

What are the limitations of team building? Change cannot be expected to occur overnight. The leader and the team must frequently evaluate the effects of the team-building workshop, readjust strategies, and reinforce positive change resulting from the team's efforts.

To insure the maximum long range results, several Agency organizations have conducted two or three formal follow-up team-building workshops and 20 or more project meetings or informal sessions. One must remember that organizational change is a very slow process and requires time to work through the action plans developed at the workshop.

SUMMARY

Team-building workshops simply attempt to eliminate barriers to collaborative behavior within the team by developing skills that foster greater team attention and direction to the achievement of tasks. Team building is based on problem-solving rather than fault-finding to promote individual and team growth. The bottom line is improved organizational effectiveness and employee satisfaction.

Team building cannot be viewed as a panacea for problems or ineffective behavior in an organization. Other factors such as the total organizational environment or culture, leadership styles of the managers, organizational structure, a willingness to change, etc., all play an important role and impact on the team's operation. Other management improvement techniques may be more appropriate in some cases.

For assistance or information on setting up team building workshops, please contact [redacted] or Charles Hall in the National Cryptologic School, E622, 968-8971s.

This article contains material prepared by Dr. George F.J. Lehner, a private consultant, for handouts in his workshops.

The following sources are recommended for additional information on organizational development and team building:

Baker, H.J.,
"The Hows and Whys of Team Building" *Personnel Journal*. 1979.

Blake, R.R., Mouton, J.S.
The Managerial Grid III-The Key to Leaders-hip Excellence. Houston: Gulf, 1985;
Corporate Excellence Through Grid Organizational Development.
Houston: Gulf, 1968.
Productivity--The Human Side.
New York: AMACOM, 1980.

Davis, S.A.
"An Organic Problem-Solving Method of Organizational Change." *Journal of Applied Behavioral Science*. 1967.

Francis, D. Young, D.
Improving Work Groups-A Practical Manual for Improving Work,
San Diego: University Associates, 1979.

French, W.L. & Bell, C.H., Jr.,
Organizational Development.
Englewood Cliffs, NJ: Prentice-Hall, 1973.

Rubin, I.M., Plovnick, M.S., and Fry, R.E.
Task-Oriented Team Development.
New York: McGraw-Hill, 1977.

Weisbord, M.R.,
Organizational Diagnosis: A Workshop of Theory and Practice.
Reading, MA: Addison-Wesley, 1983.

P.L. 86-36

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

P.L. 86-36

USER-FRIENDLY PASSWORDS (u)

CRYPTOLOG has been the forum for several discussions on passwords, most of them in the vein of "what not to do." Here are some ideas of "what to do" that have proven useful to my co-workers and me.

At one time I had accounts on a Multics system, a large IBM system, and three Unix systems, all of which required passwords. I was really tempted to use one password for all of them. But I had been trained in the military to be sensitive to avoiding the use of crypto material from one system on another lest there be compromise. So I felt compelled to find some way of keeping the passwords for so many systems separate and yet easy to remember. Fortunately for me, I shared a group account on one of the systems. The group consisted of unusual people who got involved in a "more-security- conscious-than-thou" contest which taught me something about secure passwords.

From these two factors (the need to generate and remember several passwords and my group's security contest) came two easy rules to use to make your passwords more secure and a third to make them more easy to remember.

FOR THE SAKE OF SECURITY,
use passswords that:

* ARE LONG ENOUGH (6 to 8 characters long will do); and

* CONTAIN UPPERCASE LETTERS, NUMBERS, AND SPECIAL CHARACTERS.

Using these two rules will go a long way toward frustrating an exhaustive search for your password by someone else on the system. The mathematics behind these concepts can be simplified to comparing the possible number of four-letter, lower-case words (26^4 or 456,976 -- about half a million) on the weak side against the possible number of six-letter words using upper-case and lower-case letters plus numbers and special characters (92^6 or 606,355,001,344 --

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

about half a trillion, or about a million times as many). You can see that the longer the password and the bigger the character set from which it is drawn, the longer it would take, on average, for an exhaustive search to recover passwords.

There are smarter ways to recover passwords than through an exhaustive search. An interesting experiment was conducted in the early 1980's by a system guru who got permission to check on password usage in an agency system with users scattered all over the R Organization. He wrote a routine to compare the words in the UNIX spelling checker's dictionary with the list of passwords. He found that roughly half of the passwords were dictionary words and involved only lower case letters! Worse yet, some of them were only four or five letters long. Let us hope that after reading this article you will be having too much fun to use such puerile passwords.

TRULY MEMORABLE PASSWORDS
CAN BE FUN!

FOR THE SAKE OF HAVING FUN AND OF REMEMBERING YOUR PASSWORD EASILY, DRAW YOUR WORDS FROM SOME FAVORITE CATEGORY SUCH AS BASEBALL TERMS OR FLOWER NAMES

For example, if you enjoy baseball, your password for one month might be

ball&Bat

(note the use of a special character and a capital letter). The next month you might choose

61Maris

to celebrate Roger Maris' 1961 record of 61 home runs. Next you might use

O_fever *or* **>goCUBS<** *or* **LAisBad!**

(notice the use of upper case and special characters). I have found that anything humorous or emotional is easier to remember than something bland. For example,

3Stooges

would be easier for many people to remember than

3Donuts.

Moreover, passwords that call up vivid mental images are better than abstractions. For example,

Sinatra

would be easier for most people to remember than

Vocalist.

Another way of adding fun to your passwords is to replace letters with similar-looking special characters or numbers. For example the last two passwords could be written

$!na + ra** *and* **v0{al!$ +

If you do not already know, you will have to ask someone or experiment to find out which characters --such as # and @ in UNIX--cannot be used because they have special functions. Passwords like these are harder to type but lots more fun. This element of fun helps people set aside their old passwords for cute new ones. Sometimes I can hardly wait for the month to end because I want to start using a new password I have dreamed up!

Another fine idea for secure, memorable passwords is to think of a sentence with six to eight words in it and use the first letters as the password. Using the example of my security advisor:

I have five kids too many!

would become

Ih5k2m!

When I was involved with many computer systems at the same time, I drew the passwords for each one from a different category That was the only way I could think of to keep them all straight without writing them down Once a month I would have a psychic trauma when I had to change all of the passwords, but the categories helped me keep them straight

I have found a few problems with the mechanisms built into our machines to keep them secure. On the UNIX systems I learned the hard way that I could change to a nine-character (or larger) password and the "passwd" routine would not complain. However, when I tried to log in with it the system would not accept it. I

~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

wish that both the passwd routine and the login routine would ignore anything beyond the eighth character. That way I could use my easy-to-remember passwords that exceed eight characters; the six-to-eight character range is too limited for my taste, but this is only a minor nuisance. A friend gets around this limitation by remembering to stop after 8 characters when his easy-to-remember password is too long. He would, for example, type in

BigBadWo

instead of BigBadWolf. As I said it is a minor nuisance.

Ludlow, however, goes beyond the nuisance of UNIX. For those of you who have never had to cope with Ludlow, a brief explanation is in order. In Ludlow-protected systems, the computer selects a password for the user; that is one way to keep people from using common dictionary words as passwords. The Ludlow passwords consist of nonsense syllables randomly chosen by the computer, such as:

SEN-SLES-GAR-BYJ

The combination of syllables is often hard to pronounce, let alone remember. The problem was so bad that Ludlow was "upgraded" to tell the user how to pronounce the password ("senseless garbage" in the case of the example)! Many users have developed their own technique for remembering their passwords: THEY WRITE THEM DOWN! This practice creates a different kind of security problem in place of the ones Ludlow supposedly overcomes. Worse yet, Ludlow strikes without warning. When Ludlow decides that it is time for a new password, it will cram one down your throat before it will let you log in the next time. My term for this kind of approach is "user-hostile!" Where were the Human Engineering advocates when Ludlow was developed? Ludlow is enough to make a dedicated time-sharer welcome a personal computer, even the ASTW!

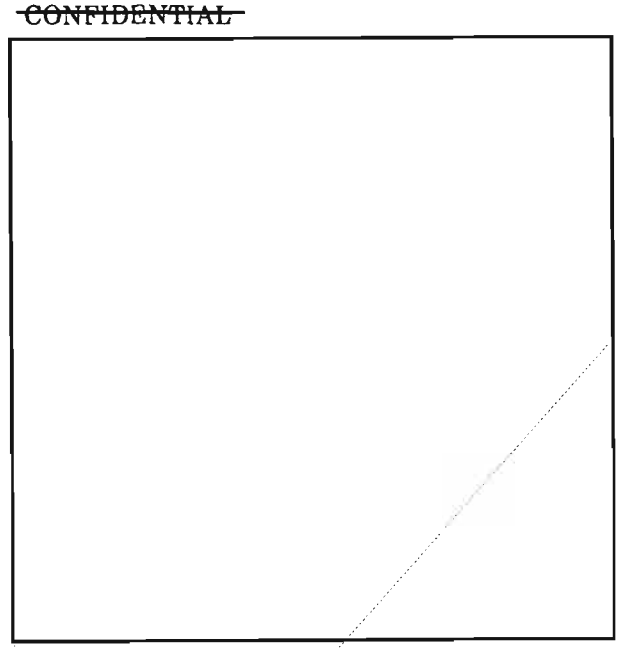
Actually, a combination of the UNIX and Ludlow approaches to renewing passwords would be more effective, secure, and user friendly. The UNIX approach is to nag the user into changing the password once the old one has gone stale, after 30 days. Unfortunately I have seen employees hardened to nagging who will put up with the UNIX reminders for extended periods rather than give up their comfortable old passwords. For such people I would like to see the reminder get some Ludlow teeth so that after a grace period the user would be forced to change before logging in. Ludlow also prevents people from engaging in the cute but unsecure practice of circumventing the UNIX renewal provisions by changing their password to something temporary and then immediately changing back to their comfortable old password.

This raises the point that no system is more secure than the way humans use it. Humans cannot design machines that other humans cannot circumvent. The people who use computers must of their own volition adhere to security procedures in order to minimize security risk. That is the main reason I have suggested these three easy rules for secure, user-friendly passwords. By making secure passwords more easy and fun, I hope to help people want to be more supportive of the security of the computers they use. □

SOLUTION TO CRYPTO-PUZZLE No. 29

(May 1985)

~~CONFIDENTIAL~~



~~(C-CCO)~~

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

DOCID: 4019705

ERRATUM

To the Editor:

I wanted to thank you for your help with my most recent article ["A Morality Play in One Act," Jan-Feb 1986], but I also must point out that the Xerox Star seems to have misplaced the various deadlines on Rosa Really's "Anatomy of a Project" chart by about 60 days each. I am enclosing a corrected version of the chart with hopes that you could publish this corrected version in the next issue.

Also, Rosa has pointed out to me that, while common usage frequently expands "PR" as "Purchase Request," the correct expansion is "Procurement Request." I have made this correction on the chart as well.

The Editor replies:

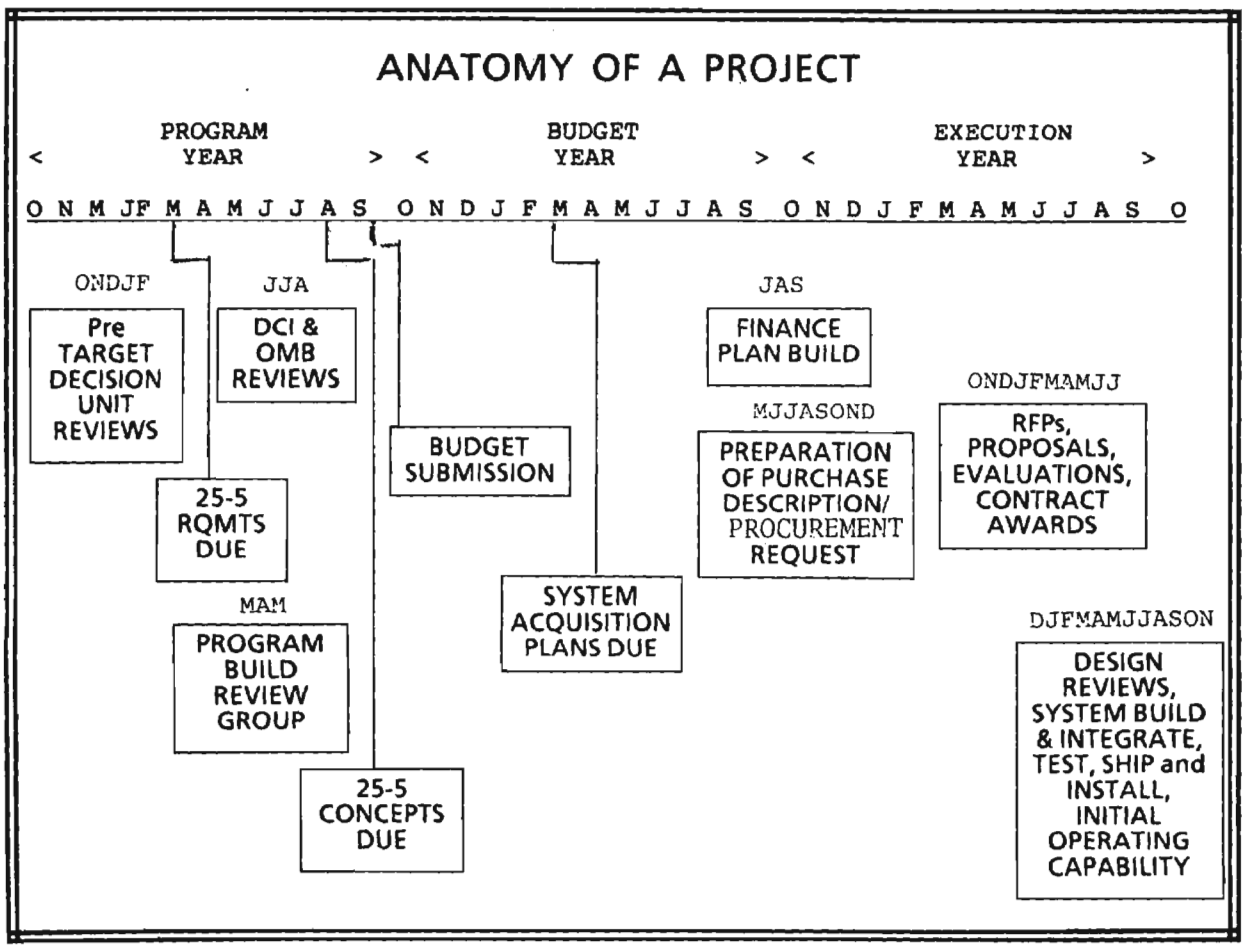
The Star apologizes for its error. These fancy word processors do take a lot on themselves !

The corrected chart appears below.

You're lucky to have Rosa and her eagle eye on your staff. CRYPTOLOG can use someone of her talents.

Any chance of borrowing her at press time?

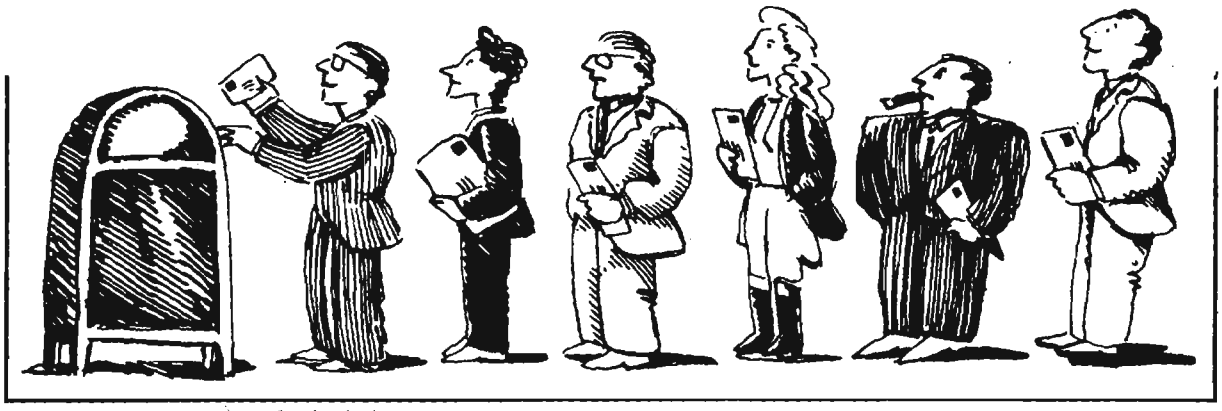
[redacted] P.L. 86-36



~~FOR OFFICIAL USE ONLY~~

DOCID: 4019705

Letters



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

To the Editor:

[redacted]

P.L. 86-36

To the Editor:

(U) Regarding the article "Why Do We Need Those Funny Alphabets?" in the November-December issue of CRYPTOLOG: the ASTW, under PC/IX, does support the 8-bit ASCII character set that was mentioned at the top of page 9. ASTW-PC/IX also supports the Cyrillic alphabet as an alternate character set. This alternate character set is accessed via the <LANG>key.

[redacted] T322

The author snarls: P.L. 86-36

(U) The ASTW can display 256 characters only by switching to the color mode (ASTW User,'s Manual, p. 17). This does not give the ASTW a full 8-bit capability, as is illustrated in Mel Deatherage's article on pp. 10-11 in this issue.

[redacted] *P16*

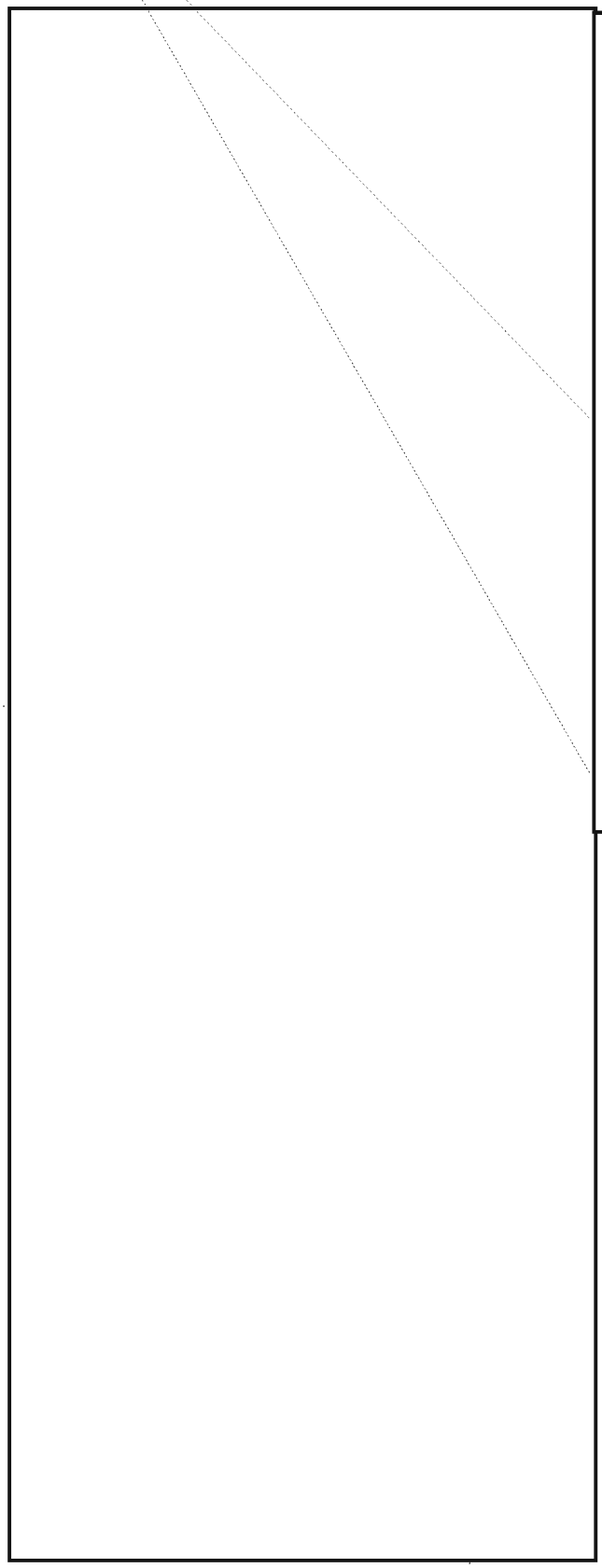
[redacted]

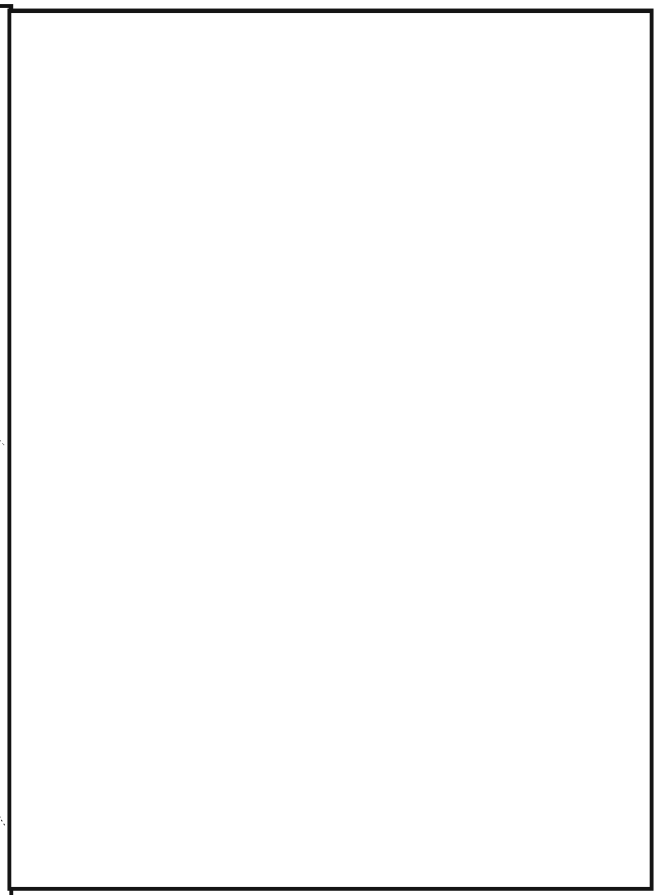
EO 1.4.(c)
P.L. 86-36

DOCID: 4019705

P.L. 86-36

~~SECRET~~





P.L. 86-36

To the Editor:

(U) Thank you for writing and publishing the help wanted ad for the SEASCAPE project. It provided an effective means of reaching the unique talent needed for the job, and opened it to a larger pool of people.

(U) The job is filled!

(U) Thanks again.

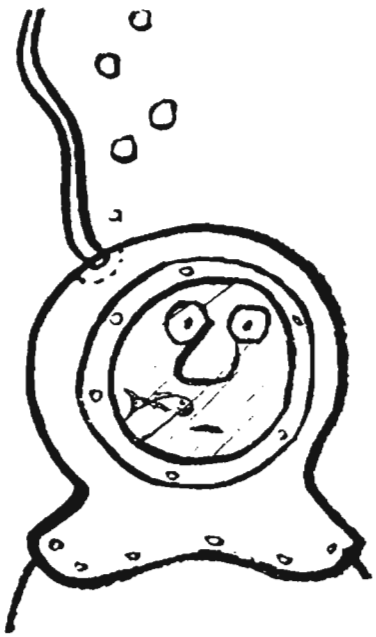
D/C. G434

P.L. 86-36

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

DOCID: 4019705

OUT OF MY DEPTH #4 (u) wes



(U) Strictly speaking, this is a puzzle only in lay terms, in that a cryptogram can be viewed as a kind of puzzle. Cryptanalysts will recognize it as a standard school exercise and may give it a miss.

~~(FOUO)~~ You are given three clues besides the line-up of the messages. One is free key (that's the digit **5** sitting up there by its lonesome). The second is the meaning **period (.)** for the intermediate plain dinome **56**. The third is the stereotypic message ending **56 = period**.

(U) If you need more to go on, write for instruction, **do not call**, to The Puzzle Editor, CRYPTOLOG, P1.

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

DOCID: 4019705

READERS' SURVEY

As an experiment we used a variety of fonts and spacings in this issue.

Which do you find easiest to read?

Please number your preferences 1-15, best to worst, and send this sheet (or a copy thereof) to:

Editor, CRYPTOLOG, P1, HQ 8A187.

___ ODYSSEY

___ EFFECTIVE C3 ANALYSIS

___ A LINGUIST MEETS THE ASTW

___ AI AT NSA

___ PRESERVING DOCUMENTS

___ TEAM BUILDING

___ PASSWORDS

ERRATUM

___ [ ]

___ Editor

LETTERS

___
___
___
___
___
___

[ ]

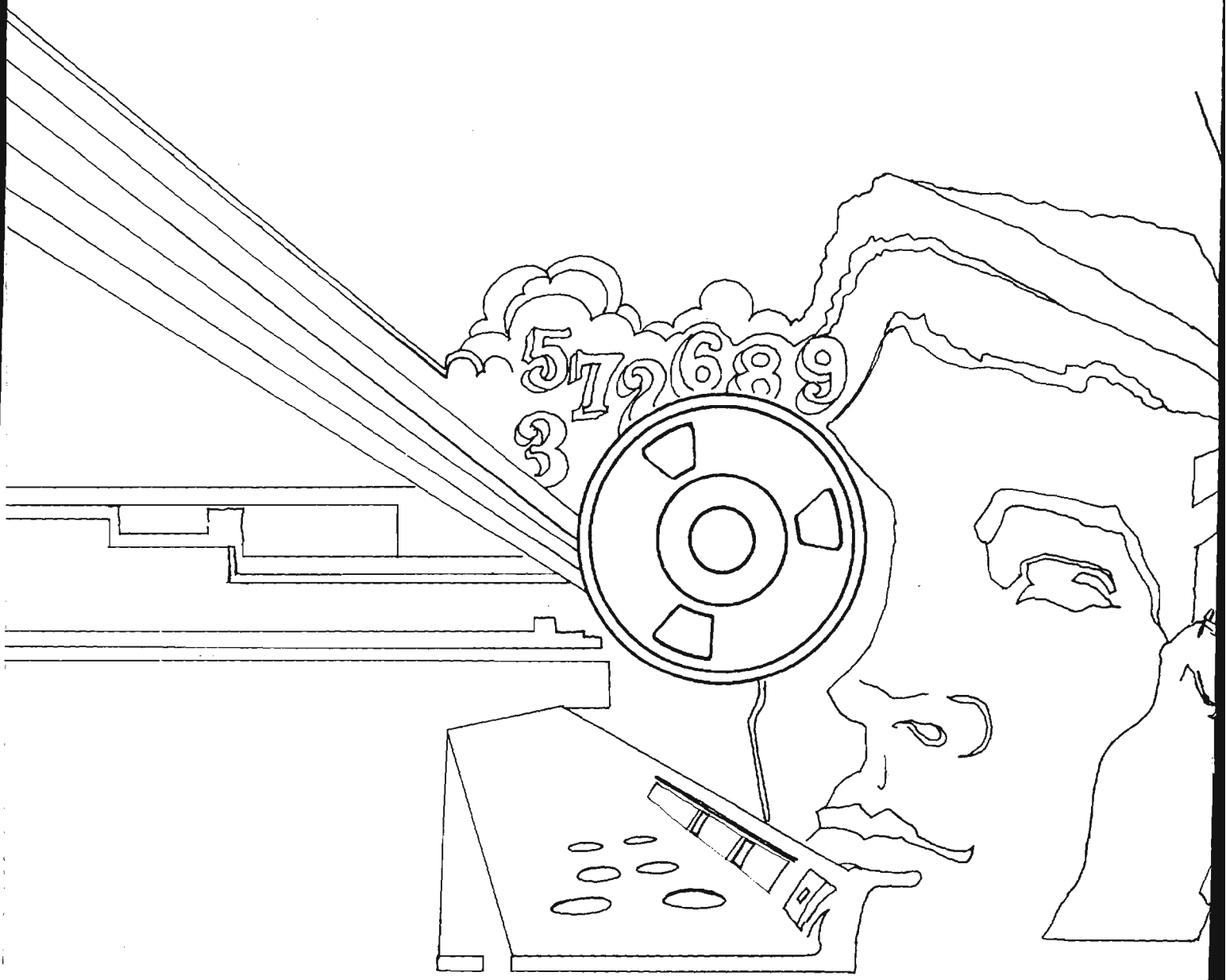
P.L. 86-36

COMMENTS

Optional: Name, Organization, Secure Phone

~~FOR OFFICIAL USE ONLY~~

P1-JUL 86-Y1-111512


5726893

This document is from the holdings of:

The National Security Archive

Suite 701, Gelman Library, The George Washington University

2130 H Street, NW, Washington, D.C., 20037

Phone: 202/994-7000, Fax: 202/994-7005, nsarchiv@gwu.edu