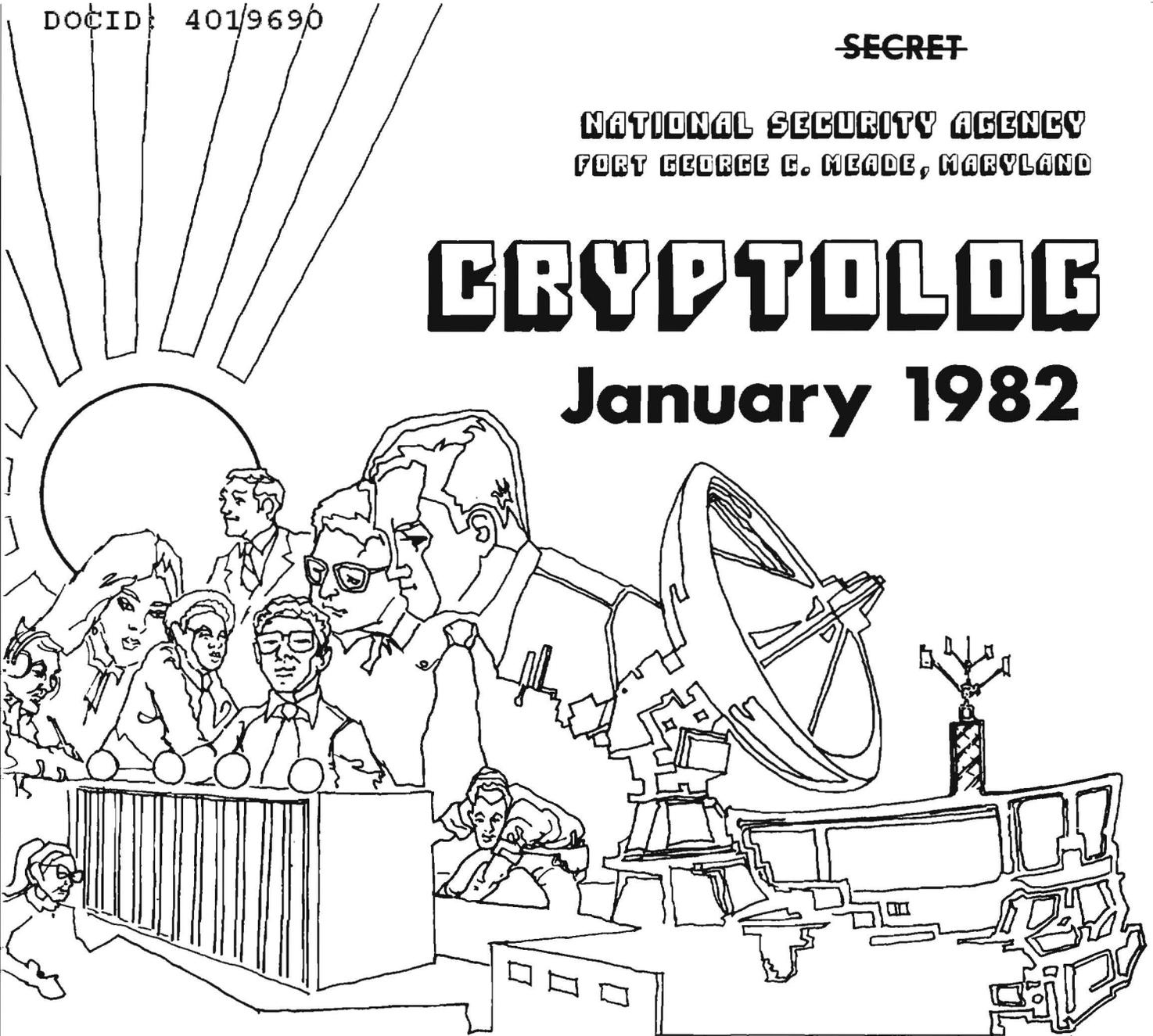


~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

January 1982



P.L. 86-36

HF - THE REBIRTH (U).....	[REDACTED].....	1
VIDEO ENCRYPTION: A REPORT FROM EASCON 81 (U)....	[REDACTED].....	4
DATA FIELD NAMING/CODING CONVENTIONS AT NSA (U).....	[REDACTED].....	5
NSA-CROSTIC NO. 37 (U).....	David H. Williams.....	14
THE LITERARY BENDS (U).....	Albert I. Murphy.....	16
ALL THE ALLIGATORS AREN'T ON SPORT SHIRTS.....		21
HUMAN FACTORS CORNER (U).....	[REDACTED].....	24
LETTERS (U).....		28

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSS 123-2~~
~~REVIEW ON 10 Jan 2012~~

CRYPTOLOG

Published by P1, Techniques and Standards,
for the Personnel of Operations

EDITORIAL

One more Agency magazine has ceased to be. The October-November 1981 issue of The Research and Engineering Review (RER 9-81) was its final issue. It seems appropriate to quote (in part) from the last editorial.

VOL. IX, No. 1

JANUARY 1982

PUBLISHER

[Redacted]

BOARD OF EDITORS

- Editor-in-Chief. [Redacted] (7119/8322s)
- Production..... [Redacted] (3369s)
- Collection..... [Redacted] (8555s)
- Cryptanalysis..... [Redacted] (5311s)
- Cryptolinguistics..... [Redacted] (5981s)
- Information Science.. [Redacted] (3034s)
- Language..... [Redacted] (8161s)
- Machine Support. [Redacted] (5084s)
- Mathematics..... [Redacted] (8518s)
- Puzzles.....David H. Williams (1103s)
- Special Research.....Vera R. Filby (7119s)
- Traffic Analysis.....Don Taurone (3573s)

"The RER was a fine idea. A need existed, and the Review filled that need well. But the declining availability of technical articles has made continuation virtually impossible.

"This problem has been growing for some time, not only for the RER but also for other NSA technical journals. Publication on a monthly basis has become increasingly difficult. The people we look to for good material are the busiest people, and we cannot question their priorities.

"Recent interviews and a sampling of readers' opinions provided no reason to believe that the future would be any brighter, and the responses showed a dwindling level of interest and support.

"We continue to encourage all of you to write for publication in NSA journals. Share your knowledge. Publicize your accomplishments."

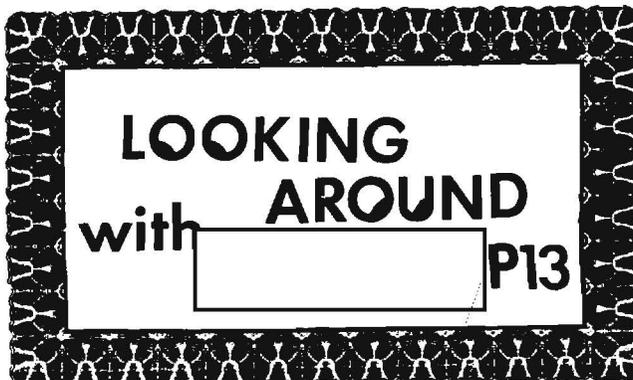
We enjoyed the RER. We are sorry to see it go.



Note:
The November, 1981 issue should be numbered
Volume VIII, Number 11.

For individual subscriptions
send
name and organizational designator
to: CRYPTOLOG, P1
or call [Redacted] 3369s

To submit articles or letters
via PLATFORM, address to
cryptolg at barlc05
(note: no '0' in 'log')



◇ HF-The Rebirth ^(u)

◇ Video Encryption:

a report from EASCON 81 ^(u)

P.L. 86-36

The Tidewater Chapter of AFCEA at Langley AFB, Virginia, held a one day seminar on the increasing use of HF and commitment of the U.S. military services to new HF systems. A number of technical talks were given on:

- the "rebirth" of HF,
- HF receiver technology,
- antenna developments,
- HF operations in the Indian Ocean,
- automatic connection of HF circuits, and
- the rediscovery of HF for C² (Command-Control).

A panel of two generals and a Navy Captain then commented on the presentations.

(U) There is high level interest in HF by OSD and JCS, and new technology, but the military services have lost their HF skills. The communications users, having accustomed themselves to the lavish services that satellites can provide, do not like to conduct their operations with narrowband HF message services. The equipment is better, but is expensive, and there is trouble getting the money. In spite of these problems, HF is seen as vital to future combat operations, because the

services cannot be sure that satellite circuits will be available.

Highlights of Discussions (U)

(U) ITT is developing a frequency hopping HF system called "adaptive HF" which is designed for operation during and after a nuclear war. It will communicate on skywave links up to 100 MHz after a nuclear event. The pulses are noise coded but the demodulation can overcome perturbations to the waveform caused by nuclear effects, and apparently does not require correlating filters at the receiver. This system will do automatic real time sounding of the ionosphere, can change its routing, and has low probability of exploitation (LPE). It is designed to provide "enduring C³" so that transattack and postattack negotiations, as well as combat C², can be carried on despite outages of other communications systems.

(U) RACAL has developed a digitally controlled HF receiver, RA 6790, which was designed to replace the R390. The receiver contains a microprocessor which controls all the functions of the receiver, including self-test. Special AGC circuits give 0 dB output variation for 120 dB input variation. The synthesizer is on one PC board and tunes 1 Hz increments across the receiver range. A wideband input circuit is used which keeps intermodulation products to a low level. A mathematical formulation was given of the distribution of weak and strong signals over a 4 MHz band, derived empirically. A RACAL 2174 receiver with many of the RA 6790 features is

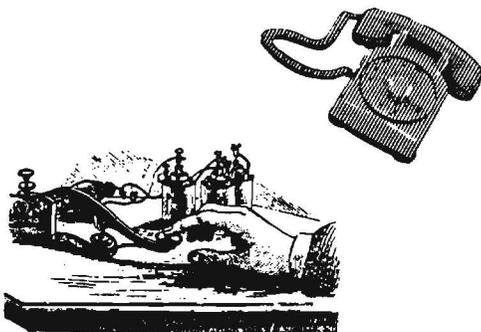
being adopted by the USAF.

(U) RSI has developed a portable microwave antenna for troposcatter or line of sight links, which can be assembled and erected by two men in 8 minutes. A demonstration was given. The antenna weighs 450 lb.

(U) BR Communications chirpsounders and spectrum analyzers are being used by the naval task force in the Indian Ocean to improve HF circuits to distant shore stations. Flag officers aboard the Mt. Whitney use a total of 29 HF circuits almost continually, relayed through Diego Garcia, Australia, Greece, and the Phillipines, even though the ship has satellite circuits. The Navy has had to redevelop its HF skills to operate these circuits, and channel sounders have enabled frequencies as high as 29 MHz to be used. Smallpipe HF exercises in which satellite circuits are turned off have exposed many problems, including long delays in delivering traffic.

(U) ROCKWELL has developed a system which will automatically set up an HF circuit to a mobile station, e.g. aircraft, and confirm the link in a few seconds, then terminate the circuit when the message is complete. Voice can be used after setup. They have also developed an HF 80 series of equipments for the military communications market.

(U) The Navy, having dropped HF communications about 10 years ago to switch to satellites, is now encountering problems in going back to HF. The experienced people are leaving or retiring, and the operators familiar with satellite circuits have to be retrained for HF. Special problems such as the "rusty bolt effect" have reoccurred and have to be solved again. Lengthy messages also overload HF circuits without conveying information quickly.



(U) Captain Gradel, USN, said, in a comment, that the Navy was having trouble getting money for HF, and the commanders who have gotten used to the benefits of wideband satellite circuits do not want to operate with only HF circuits.

(U) MGen Ray, USAF, commented that USAF was unwise in giving up HF, and JCS and DCA now want HF. RDF contingency plans are dependent on HF. USAF is ten years behind the Navy in use of chirpsounders.

(U) MGen Gray, USMC, commented that the Services had to retain their "institutional memory" of operational knowhow as personnel changed. HF communications were important to the USMC, which he thought was likely to be in combat in the 1980's. HF was used for short range ground wave as well as skywave communications. Combat conditions would require use of NBC (Nuclear-Biological-Chemical) gear, and HF equipment would have to be useable in that environment. Messages would have to be concise. Cost and weight of equipment was important, and only equipment actually in hand could be used.

(U) Other points learned from the discussions:

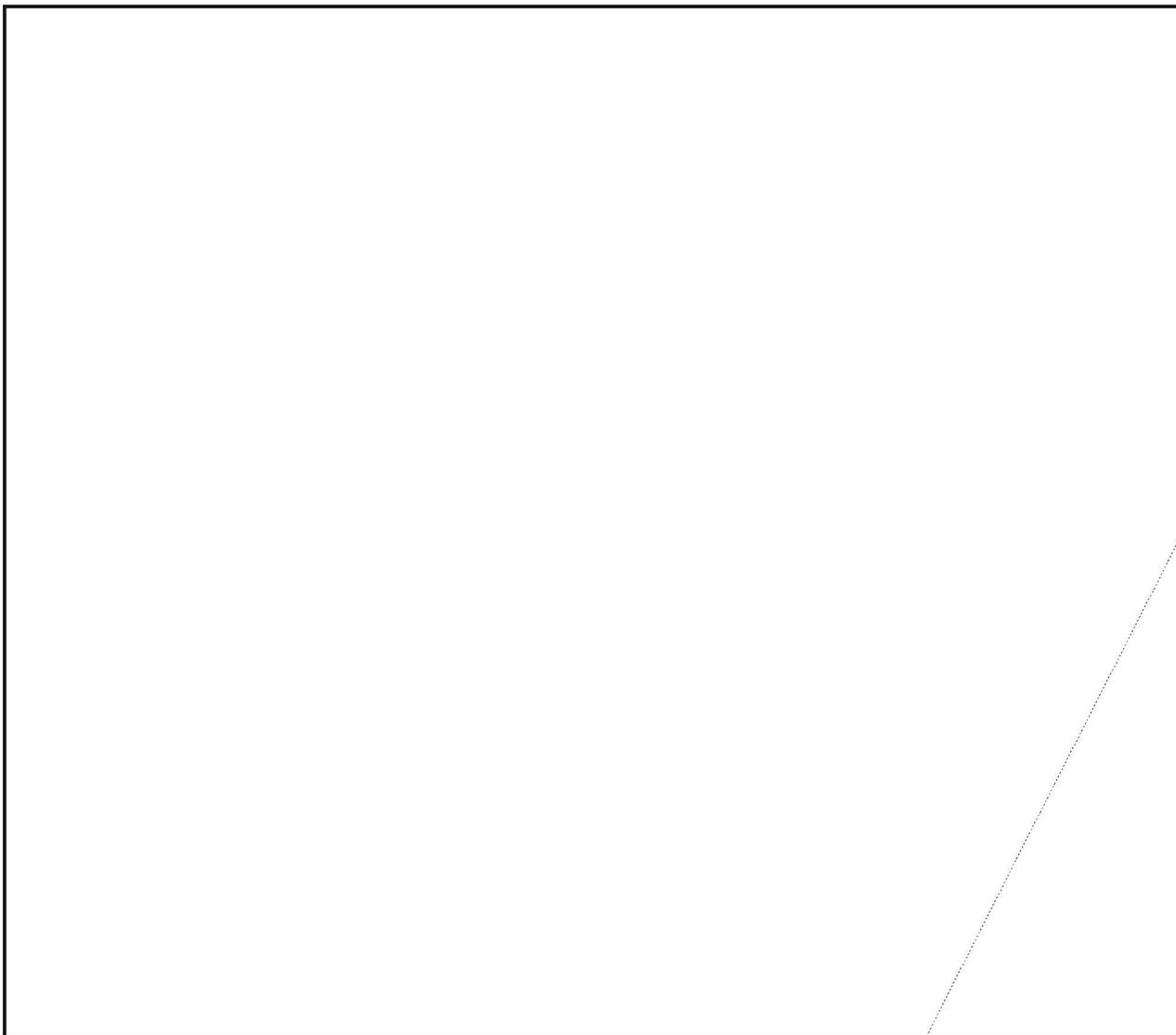
- ★ US communicators use CW Morse at times, and tune RTTY transmitters off assigned frequencies in order to overcome cochannel interference, which is severe.
- ★ In this CW mode, operators use "fist" recognition to set up their nets.
- ★ The military services will not give up their HF frequencies.
- ★ Third World countries will probably use HF whether they get frequency assignments from the ITU or not.
- ★ High bit rate systems, above 300 bps, are thought unreliable because of the prevalence of cochannel interference which degrades demodulation.
- ★ The military services will have to retrain operators for HF, and may maintain a minimal CW Morse capability despite higher automation.

- ★ Usage of the 20-30 MHz range, and use of "open" frequency channels on an opportunistic non-interference basis, is expected to grow.

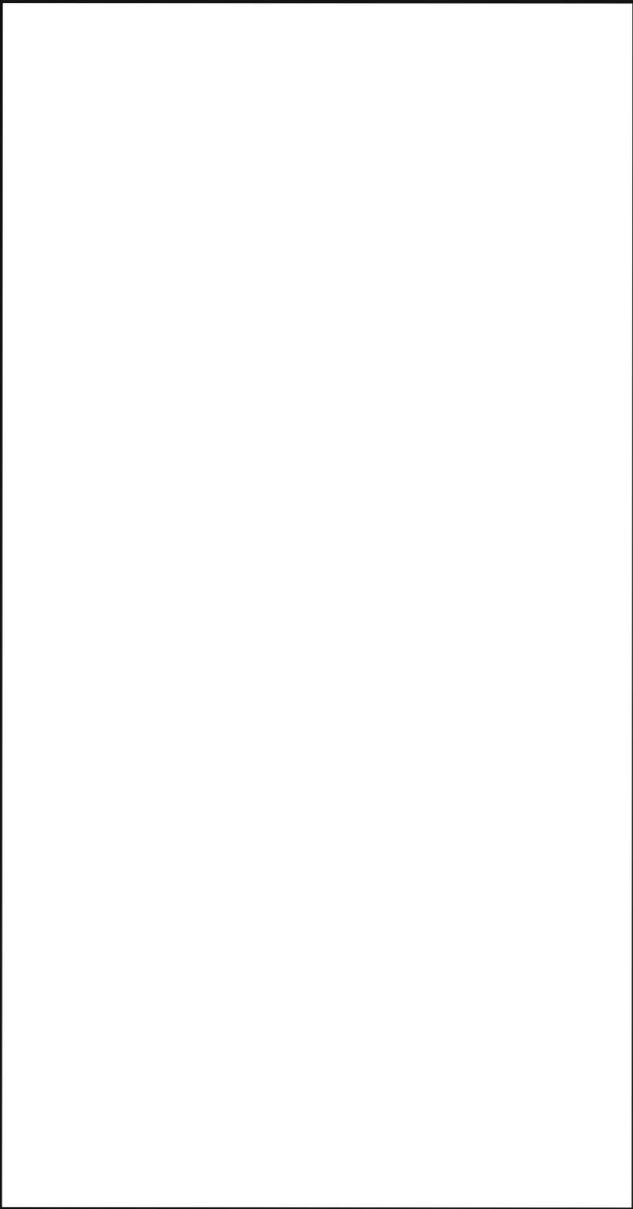
(U) The reported "death" of HF has been greatly exaggerated. Its use has continued to grow even though the U.S. Services largely switched to satellites. Important high level traffic for U.S. military and diplomatic users will pass over HF in peace or war, complementing satellite circuits. The U.S. military "rebirth" of HF usage is taking place in a changed and more congested environment, with moderate technical improvements in equipment, but major training and adjustment problems must be solved.



Cryptologic Implications ~~(C)~~



~~SECRET~~



highly secure. OAK Communications has a changing video analog encryption in which the enciphered keys are sent in band with the signal. The encryptor is called ORION. The video security is "soft", the audio security is "hard" and the decoders will sell for about \$2000. HBO, in circulating a new specification for quotations, found ten suppliers from CATV, Broadcast and "Military" willing to bid. COMTECH Communications Corporation has a system that will give "hard" audio encryption, possibly using DES, and "medium" video encryption. Their security is based on a proprietary integrated circuit which keeps the encryption technique under their control. They can accommodate 60,000 subscribers with one PN sequence, and can rekey outstations at 20,000/minute. Individual subscribers can be turned off if desired.

~~(FOUO)~~ The speakers were extremely secretive about specific techniques. The remote keying scheme developed by NSA in the 1960's appears to be the basis for the systems, since the broadcaster can control all the outstations in case they do not pay their bills, or decoders are stolen. The fast rekeying, and the ability to select individual sets out of the net are significant. Audio encryption will be at least at DES level. Subscription over the satellite links will be numbered in thousands of ground stations. The systems will also provide video conference capability. Video quality must be of studio quality after decoding, for the pay TV customer. The DIGITEL CANADA technique, which uses digital encryption and analog transmission, with sampling at 14.3 MHz, may be the most novel and secure.

~~(FOUO)~~ The consequences of these TV encryption projects will be to put secure remote keying networks systems into the market at about \$1000 or less per terminal.

EASCON 81: Video Encryption

~~(C)~~ Encryption systems for satellite distribution of TV video and sound are advancing rapidly, especially in the command-control and remote rekeying of the decoders. The new HBO (Home Box Office) specification will use a key generator of DES security or better. DIGITEL CANADA has a prototype of a digital encryption system for high quality video which can be sent within a TV₁₃₉ baseband. Their picture encryption has 10¹³⁹ ways to encode. They can rekey subscribers at 2200/minute, and remotely terminate any unit. Both video and audio are



~~SECRET~~

~~CONFIDENTIAL~~

Good Grief, Charlie Brown, Not Again...! (u)

Data Field Naming/Coding Conventions at NSA (u)

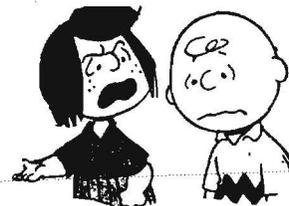
by P13

This paper is intended to be a "primer" on some of the basics of data standards. My main purpose is to shed some light on the conventions ~~(FOUO)~~ that exist at the Agency concerning the naming and coding of data fields. Yes, there are conventions in this area of data processing, conventions which sadly are much more honored in the breach than in the observance. And yes, the Agency does have an official policy on the subject. It is pretty much buried in the pages of a USSID (414) and an NSA Reg (80-9), and ignorance about it is rife (I'm afraid) among the DDO analysts whom it chiefly affects. However, it is a policy that makes a lot of sense, especially as we view the Agency moving steadily into a world of proliferating data of all kinds -- files, programs, data elements, and data fields, and all of them sprouting wildly and threatening rapidly to grow out of control. Happily, we have some good things going for us. PLATFORM is one. A centralized DDO Data Element Dictionary/Directory is another. (It is still in the embryonic stage, but it offers hope for the future.) But before we can manage and exchange our data efficiently, we have to apply precision and consistency to the practice of identifying the data elements/fields making up those burgeoning data bases. Literally, we have to get a better handle on our data.

~~(FOUO)~~ What after all is the lowest common denominator, or lowest information level, of the vast data banks that fill our computers and memory devices? Undoubtedly, the Data Element itself, which can be broadly defined as the most basic unit of information. And since the Data Element (or rather its data items) is the entity that inhabits the fields comprising those miles of data banks, it seems reasonable for us to consider carefully how these data fields are to be addressed and referenced.

CLASSIFICATION NOTICE:

Although each individual paragraph in this article is unclassified and handled as "For Official Use Only," the compilation of the information presented in its totality is classified ~~CONFIDENTIAL~~.



P.L. 86-36

~~(FOUO)~~ A brief look at the origins of the data standardization program at NSA may help set the stage for this discussion. We will then look in some detail at the two chief ingredients that are mixed together to affect the process of naming and coding data fields, namely, the Data Element and its companion, the "Data Use Identifier."

Origins of the Data Standards Program (U)

~~(FOUO)~~ The 23rd Anniversary of Pearl Harbor, December 7, 1964, was a landmark date for Department of Defense efforts to get underway with an organized effort in the field of data standards. On that date, DoD Directive 5000.11 established the "Department of Defense Data Elements and Data Codes Standardization Program." Several months later, on 12 March 1965, the Assistant Secretary of Defense (Comptroller) sent a memo to DoD components entitled "Data Elements and Data Codes Standardization Procedures." (This was the draft version of DoD Instruction 5000.12, which became the bible for the DoD program.)

~~(FOUO)~~ On 3 August 1965, further guidance was offered by DoD, especially concerning criteria for standardization; for example, the requirement that each Data Item under a given DE be mutually exclusive, with no overlapping or duplication. In this regard, a Data Item was defined as "the smallest subunit or piece of information . . . which cannot be further subdivided and retain any significant meaning." Interestingly, this early document from the Defense Department emphasized the importance of Data Use Identifiers in the business of data standardization; it pointed out that they:

▶ Must have unique names;

~~CONFIDENTIAL~~



Are always reported and recorded in terms of the same Data Items and codes as the Data Element itself. (This observation is a good one to keep in mind in maintaining the clear distinction which should exist between Data Elements and their modifying Data Use Identifiers. We will look at this distinction in more detail later.)

~~(FOUO)~~ In the meantime, NSA had begun to get its own program untracked. D54 had been serving as the point of contact with DoD and had been coordinating our exchanges of ideas and problems with them. On 28 January 1965, a memorandum from General Davis, then ADP, broadened the base for data standardization within NSA and beyond. It designated PI as the "authority in P for the development and maintenance of standards for those terms which constitute elements of the technical data base for P." He assigned PI the task of developing standards in such areas as intercept coverage accounting; the data required in machinable technical reports; information in such data bases as TIPS (Technical Information Processing System - still operational); and "data comprising any similar data base or program in the future." Gen. Davis' memo spoke strongly about the desirability of achieving standardization which would relate to data bases throughout P "and indeed the entire SIGINT community." He pointed out the need for standardization in relation to:

- ★ A standard name for each Data Element concerned;
- ★ An agreed-upon meaning for each individual DE;
- ★ A body of Data Items, or the information content of each Data Element; and
- ★ A standard configuration for the DE; that is, like data expressed in a like manner.

~~(FOUO)~~ Two other documents are of interest as a background to the NSA program:

- Bureau of the Budget Circular No. A-86, Standardization of Data Elements and Data Codes in Data Systems, dated 30 September 1967, which:
 - established the Federal program for data standardization;
 - defined Data Elements and related features in terms much like DoD's and NSA's; and
 - confirmed the "cryptologic waiver," which meant that NSA would be exempt from having to observe a Federal standard which might adversely affect our cryptologic activities.
- DCID N. 1/15, DATA Element and Code Standardization for Intelligence and Intelligence Information, dated 14 October, 1969, which established a policy promoting the use of data standards in the exchange of intelligence information among information-handling systems.

~~(FOUO)~~ In developing its own data standardization program, NSA has remained faithful, with only minor variations, to the general concepts, terminology, and set of definitions passed down from its big brother, the DoD. One of these "minor variations" concerns the scope of the "Data Use Identifier" (DUI). The DoD usage has historically viewed the DUI as virtually synonymous with "Field Name."

~~(FOUO)~~ The latest editions of both the DoD and DIA standards manuals still use the term with this original meaning. In Cryptologic applications (as opposed to personnel, logistical, financial, etc.) at NSA it has been applied somewhat more narrowly than the DoD usage, i.e., to point just to the specific use of a given Data Element in making up a field name; for example, in "Date of Intercept", the phrase "Intercept, of" is considered to be the DUI. In this paper, "Data Use Identifier" will have this more restricted meaning.

The Data Use Identifier (U)
A Basic Tool

~~(FOUO)~~ The thing we data standards people call a "Data Use Identifier" (DUI) has long been a puzzlement to many otherwise well informed NSA analysts. At least such has been our experience at the Data Standards Center, where we have seen many DUIs aborted, mangled,

or otherwise abused as they drift across our desks in the form of Computer Record Formats and other EDP file descriptions. There are many reasons for the lack of knowledge as to what they are and how they should be used. One is the widespread shortage of guidance in this area, for which we at the NDSC have to bear our share of blame. In fact, the only explanatory material about DUIs readily available lies within the pages of official directives, such as the Department of Defense Instruction 5000.12 which, in April 1965, established the policies and procedures governing the DoD data standardization program, NSA Regulation 80-9, and our own USSID 414, which is the official directive for the NSA program. Very often such directives are the last thing people consult, especially when they are hurrying to get their machine projects off and running. Recognizing that DUIs are an important aspect of the business of labeling and naming data fields, the Data Standards Center is developing a working aid which lists and defines the individual Data Use Identifiers that have been standardized to date and at the same time explains how each one is used. (More on this "DUI Registry" below.)

~~(FOUO)~~ As an NSA analyst you are apt to be somewhat skeptical about this feature of the NSA standardization program. What do these "identifiers" have to do with the practical problems of managing a data file, and of what real value are they? Well, a lot, we think - if you happen to have a new file ready for machine processing and need to come up with meaningful names for what is in it. If the file is just for you and your work center alone, a private domain so to speak, then you can probably in good conscience invent your own mnemonic codes or tags and name the fields anything you like. If your file is to be shared or exchanged with some of your fellow employees, however, it is the proverbial horse of a different color. USSID 414, bearing the unwieldy name "Standardization of Data Elements and Related Features for SIGINT Activities," says, among other things, that there is a right way, and many wrong ways, to approach the problem of naming and labeling your data fields. The Data Use Identifier (which is one of those "related features" dealt with by USSID 414) has a lot to do with that right way. There is no need for us to stress the many advantages which accrue to files (and to their managers) which follow these procedures; chiefly, the fact that the name of the field and its coded representation should immediately tell a user what type of information is in it. (If they don't, we may have problems deciding what it is and whether we can use it.)

What is a Data Element? (U)

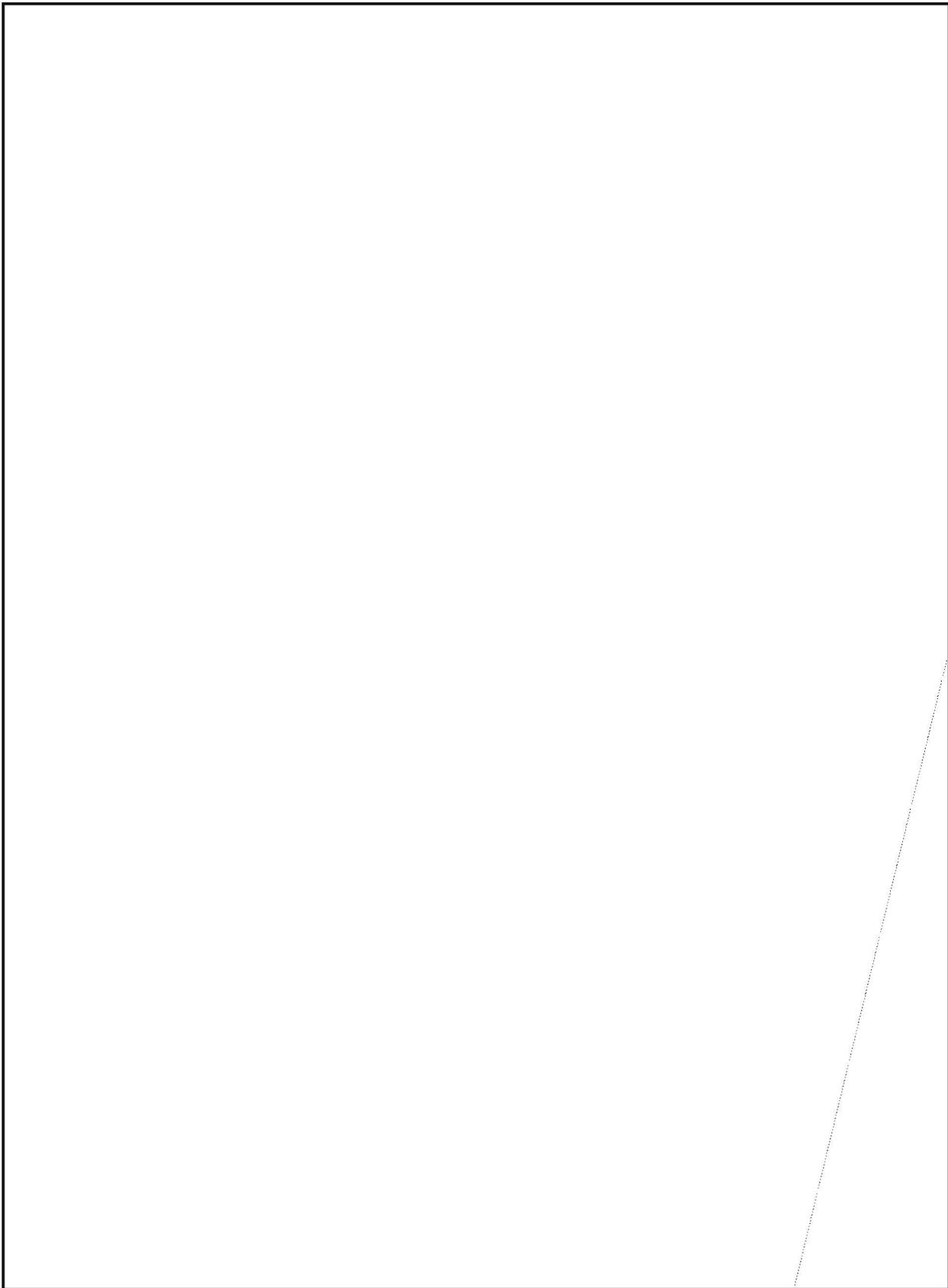
~~(FOUO)~~ Before explaining how DUI's relate to Field Names in EDP applications, we had better clarify the concept of "Data Element." The official definition, from USSID 414, says that a Data Element is a "unique grouping of related informational units." Funk and Wagnall's Dictionary of Data Processing brings in the concept of "Data Items" in its definitions:

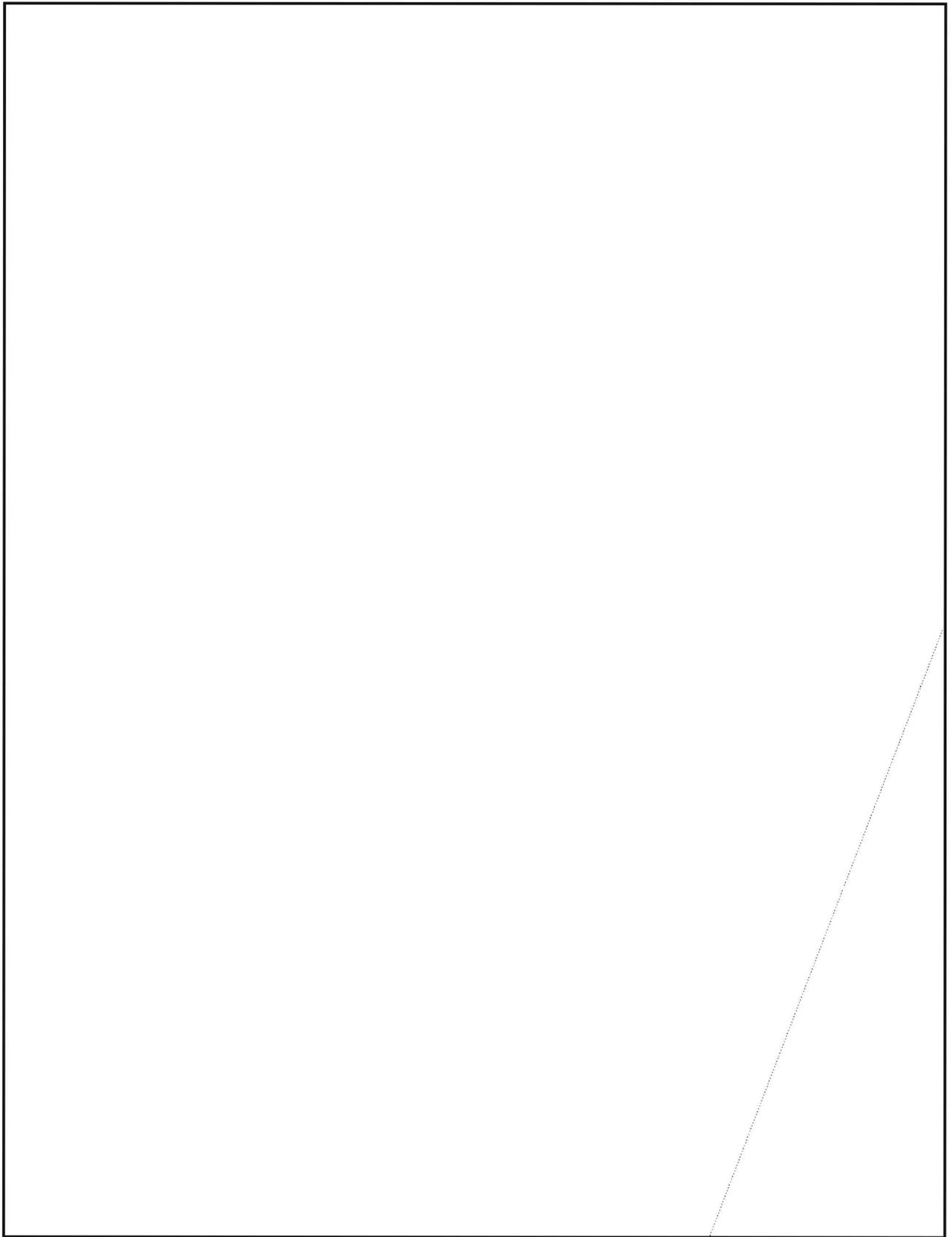
- "Data Element: a class or category of data based on intrinsic or assigned relations between data items."
- "Data Item: any individual member of a Data Element."
(One should note that a Data Item and its code are not identical.)
- Data (Item) Code: A set of characters structured in such a way as to represent the data items of a data element." (Italics mine.)

For example, "Month" is a Data Element; "January" is one of its Data Items; and "01" is the code which represents the data item "January."

~~(FOUO)~~ You can think of a Data Element as a somewhat abstract category or class of information, and a Data Item as one of the specific values that can be assigned to that DE. The set of values can be either finite or infinite. For example, "Month" has only 12 possible Data Items; "State of the U.S." has exactly 50. "Date" on the other hand has an infinite set of possible values. ("24 January 1980" is one possible Data Item; its coded representation is "800124".)

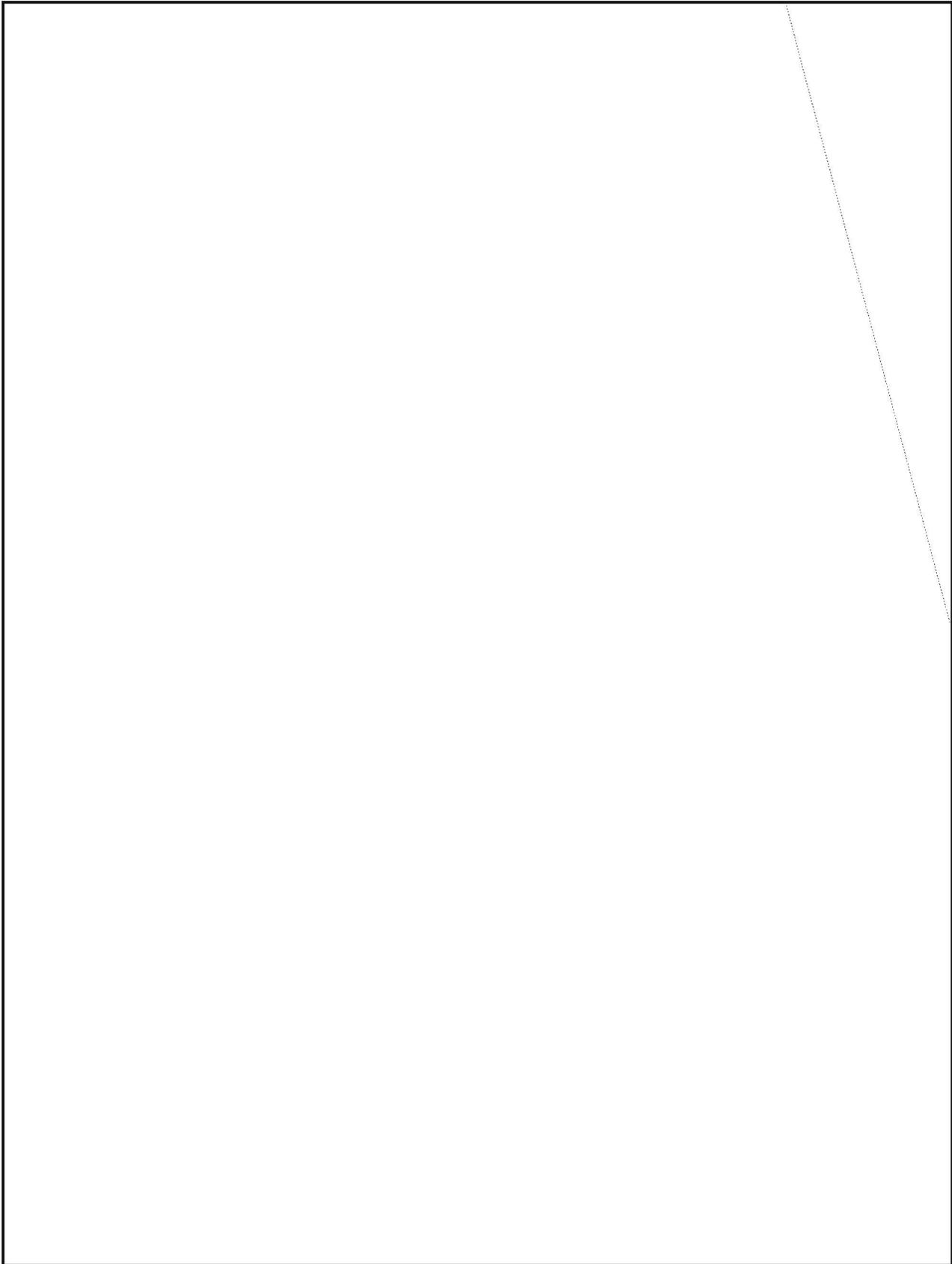


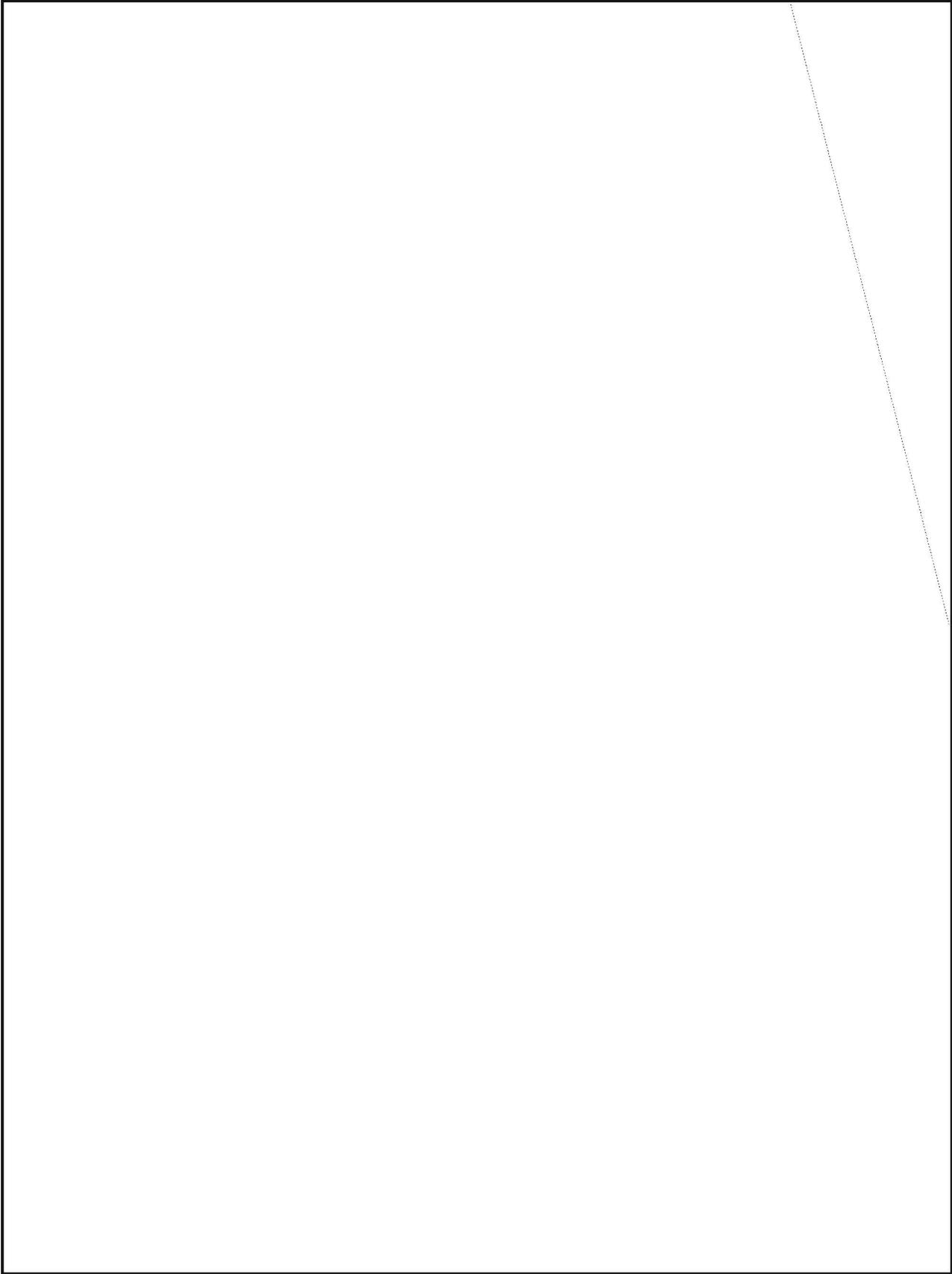










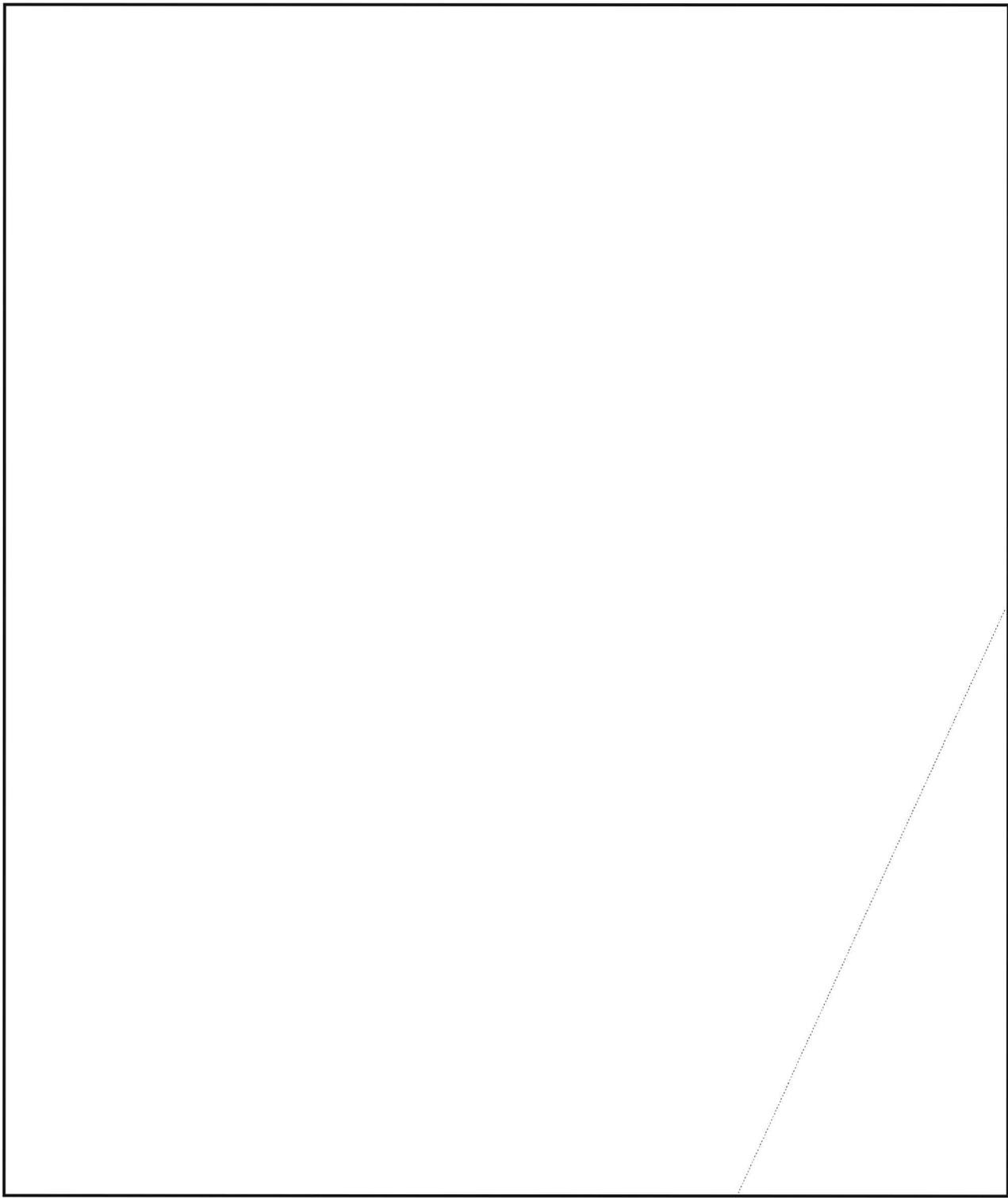


A bit of airline trivia to start the new year

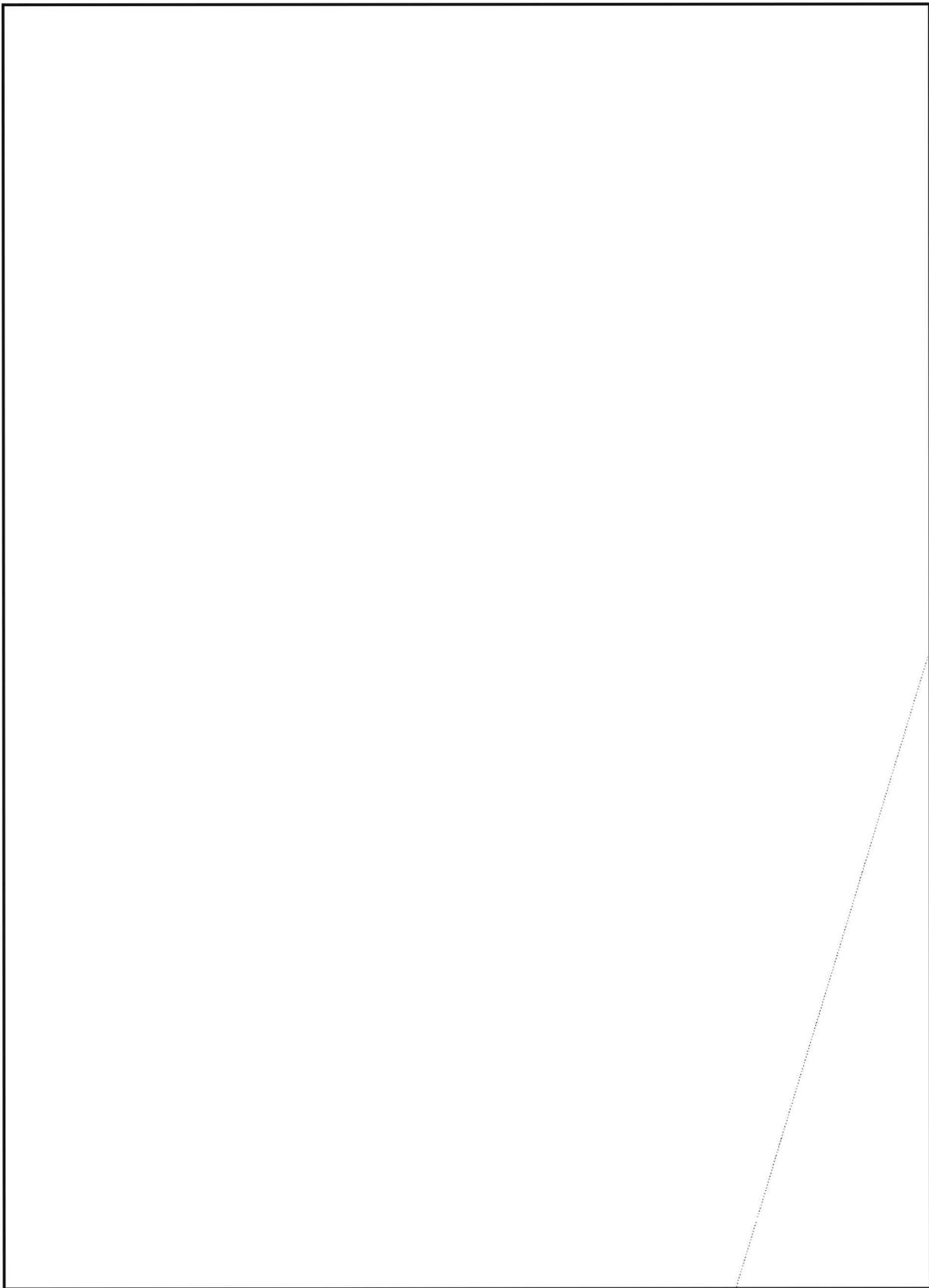
NSA-Crostic No. 37

"SAY! ... THESE NEW FLAGSHIPS
LOOK LIKE THE 'HINDENBURG'
WITH WINGS ..."

—From a 1936 ad

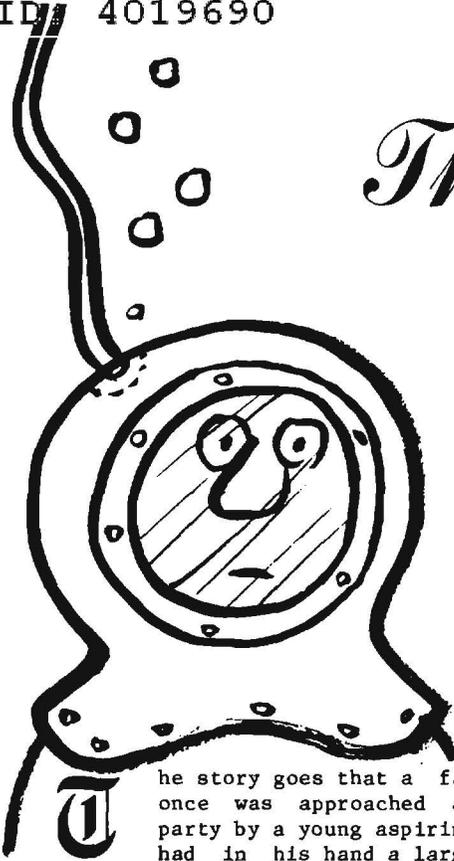


UNCLASSIFIED



8

UNCLASSIFIED



The Literary Bends ^(U)

by Albert J. Murphy, E41

The story goes that a famous author once was approached at a cocktail party by a young aspiring writer who had in his hand a large draft of a novel he had written. The young man, perhaps more brash than polite, asked the author to take the draft, read it, and suggest a title. The author, taken aback by such directness and by the size of the document, thought for a moment, then asked: "Do you mention drums anywhere in the story?" "No sir," replied the young man. "Do you mention trumpets?" Again, "No sir." The maneuver had worked. "Then why don't you call it 'No Drums, No Trumpets'?"

(U) In the business of teaching Introductory Writing (EG-022) and Expository Writing (EG-122) at the National Cryptologic School (NCS), we have encountered some rather pointed feedback from some of our students, which cannot be so easily put aside. The students talk of two worlds of writing at NSA: the ideal world of writing as taught here at the school, and the real world of writing as practiced on the job. Eventually, one of them will crystallize the issue by saying, "This course is all well and good. But when I finish it, I know I'm going to be faced with the decision of writing your way for the sake of good writing, or of knuckling under to my supervisor's blue pen for the sake of my next promotion." Rightly or wrongly, the haunting question inevitably comes to mind: "Is his or her supervisor under 35 years old and a product of society's convulsing educational system?" We choose never to ask it.

(U) How valid are these rumblings? What is the extent of alleged shortcomings in the way people in management write (we're talking primarily about supervisors and staff editors)? And what are we going to do about it? Based on our own collection of bits of evidence, coupled with this human testimony from the students, we believe that the rumblings have some validity. But since we have neither the mandate, nor the resources, nor the time for a thorough research effort, the best we can do is to present the problem in this vehicle in the hope that the managers in question will read it and do something about it.

(U) Just before the students complete our courses, as part of a normal procedure we alert them to the post-course period of what we call "the literary bends," during which they might find it difficult to apply their newly acquired (or their refreshed) set of rules of good grammar and effective writing. "Don't be surprised," we tell them, "to find your pencil frozen in your hand or your fingers immobile at the typewriter during your first writing tasks on the job." They understand that. Some have reported that that's exactly what happened. Others have had to wrestle with the problem while still in the course. It is unfortunate, however, that we are now compelled to warn them of possible additional difficulties that can occur when a person in the supervisory chain, whether through ignorance, or obstinacy, or, alas, because of misguided pressure from a supervisor at yet a higher level, discourages the students' attempts to apply what we have

taught them.

(U) If managers are willing to face up to the reality that some of their people are frustrated in their jobs because, as they perceive it, we don't practice what we preach in the field of writing, then we are well on our way to solving the problem. Perhaps, then, our message to managers ought to be --

Managers:

By all means enforce good quality control; but in the process, please be aware of this problem, be fair with your people, and be square (that is, be traditional) with the language.

We contend that the modernists are wrong. Like it or not, there is an English Language; and it is governed by a set of rules for correct grammar, effective sentence and paragraph structure, and good writing style. Perish the thought of Congress wanting to change the words of the Constitution to accommodate modern linguistic happenings.

(U) You managers, if you are following this discourse in earnest, should be asking at about this point, "Well, what have you been telling our people in your classes?" Our answer is that we've tried to convey to them the fact that there is beauty in our language, and that the students should find it and use it. We have found that they not only are receptive to this idea, but also at times are resourceful (and not too subtle) in expressing their endorsement. You can experience intellectual beauty, we once told them, by merely pronouncing the names of tribes of American Indians, for they have a majestic quality that evokes, through vivid mental picture of frontier days, much of what is noble in the American character.

Cheyenne...Pawnee...Apache...
Comanche...Sioux...Shoshone --

here the students joined in --

Mohawk...Cherokee...Blackfeet...
Chippewa...Algonquin...Iroquois.

Then the spell was broken as quickly as it began when one of the students wistfully offered...the Washington Redskins. We have told them about the importance of good communication, whether in face-to-face conversations, on the telephone, or in writing; and of the potential disasters of failing to communicate. We've advised them not to write without good reason. But once they've decided to write, they should spend some time thinking about what they want to say before committing

their thoughts to paper. They've heard us say many times that bad writing is usually the result of poorly thought-out ideas.

Grammar, Spelling and Punctuation (U)

(U) We have compiled an array of real-world writings from NSA in-house correspondence and CRITICOMM messages, which we contend are inconsistent with what we teach. But, in order not to raise the hackles of a lot of people, we will cite only a few that are important to the point we are trying to make, and then only when we think they will do no harm. Recently, E asked various in-house elements to submit any comments they might have on an NCS course on reporting, which some of their people attended. It was a bit disconcerting when a staff editor of one of those elements, in his responding memorandum, said, "We don't need grammar in the course. We in the editing chain can handle it." Impertinent of us to mention this, you say? Well, maybe. But what about the problem of credibility? It's there, isn't it? If the element in question recognizes its handiwork here, we hope the people involved will not take umbrage, but will view it in the spirit of light criticism and let us make our point. We have taught our people that

1. Dangling and misplaced modifiers are major causes of confusion in communication; to wit, "The second child, Nancy, was the only child of a mother who was divorced in her infancy"; and "If found guilty, the Division of Motor Vehicles will be notified and your license may be subject to suspension."



2. Pronouns must agree in number with their antecedents. A certain ABC television reporter either didn't do his homework or decided to go modern when, in describing a recent hurricane, he said: "Damage will be in the millions, but only one person lost their life."
3. Billy Kilmer used incorrect grammar in his beer commercial when he praised his beer for having less calories. He should have said fewer calories because few(er) is used with things you can count, and less is used with things you cannot count. ("If there were fewer TV's, there would be less noise.")
4. A writer can quickly reveal himself as less than professional if he is careless with spelling. Consider the following statement that appeared in a real-world NSA CRITICOMM message:

"SGT (John Doe) IS REQUIRED TO BE INDOCTER-NATED FOR (special clearances) PRIOR TO DEPARTURE FROM YOUR STATION."

An astute, post-publication (unfortunately) comment written across this gem facetiously noted that "This will hep with hes clarence." Also, we've made it known that irregardless is a self-contradictory non-word, despite the regrettable fact that it is listed in Webster's New Collegiate Dictionary.

5. A comma is required before and when presenting a series of more than two items (matrix, row, and column). One of our students described in class how he was rebuffed by his supervisor for insisting on applying this rule. We suggested he have his supervisor call us to talk about it. We are still waiting for the call.

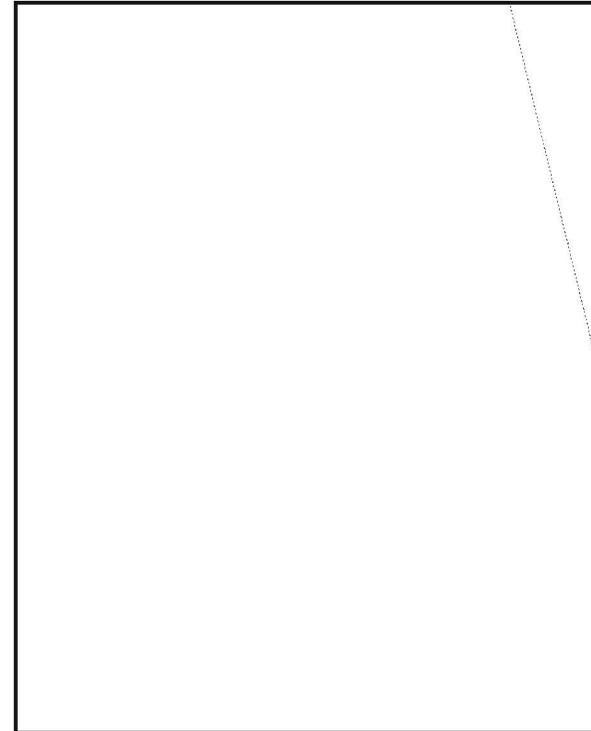
Managers:

When your people try to apply the rules of good grammar, spelling, and punctuation in their day-to-day writing, they are not trying to out-write you. They are only doing what they learned. So please -- let them.



The Sentence (U)

~~(S)~~ Since your people are not as gifted as General MacArthur was, we have trained them not to write long, Aristotelian sentences. So, when you see them trying to limit their sentences to about twenty words or fewer (to the fullest extent that the content will allow it) -- let them. We've talked them into it. Consider the following long, but not necessarily Aristotelian, opus that appeared in an out-going NSA CRITICOMM message:



We suspect that a period (a full stop) might have been intended after the word producer on the tenth line, but it wasn't evident in the copy of the message we hold. Even if the period had been inserted, the latter sentence, containing at least 105 words, would still tax the patience of the reader.

(U) In order to compose good, expository sentences, our students are following the FACTS formula (the Fast, Accurate, Concise, True, and Simple way). That means they will be trying their best to use the active voice (instead of "the great evader") and a lot of concrete, one-syllable words (we just can't bring ourselves to say "monosyllabic" as opposed to "polysyllabic" in this context). We hope we have burned ⁽¹⁾ into their memories the Lensear Write Formula which encourages short sentences, the active voice, and one-syllable words. If you ask them about it, the

chances are good that they will be able to recite to you the clear and simple "something special" lead that an obscure reporter wrote on the death of Samuel Clemens in 1909, which must have caught the breath of all who read it: "Tom Sawyer and Huck Finn are orphans tonight. Mark Twain is dead!" Notice the number of one-syllable words.

(U) We encouraged your people to use parallelism correctly and wisely in their writing, to incorporate an effective blend of periodic and loose sentences, to show their maturity in the use of subordinate clauses, and to include in their list of writing "don'ts" the principle that smothered verbs (strong verbs turned into weak nouns, such as -ization, -ment, and -ure words) and passive voice constructions frequently go hand-in-hand. The poorly written sentence "The specialization of many professions is necessitated by the complexity of our society" is best recast to read "Many professions must specialize because our society is complex." The finest sentence that we've come across at the school so far, in terms of sound structure, clear and simple content, and, yes, downright beauty, was written by a student in her autobiography project. She wrote, "When I was little, my father often said that I was the best door slammer this side of the Mississippi River." Is there any wonder why we abhor the likes of the sentence "The possible appearance of a new communications network was observed...."?

Managers:

When your people try to write in clear, simple, and direct language, don't assume that they are undereducated. They're only doing what they learned. So please -- let them.

The Paragraph

(U) We have practically ordered your people never to settle for a paragraph that doesn't have the standard properties of UNITY, COHERENCE, ADEQUATE DEVELOPMENT, and CONSISTENT and APPROPRIATE TONE. Unity calls for one central idea and a single topic sentence; coherence -- the paragraph form -- is the writer's sequence of thought from one sentence to the next, which he achieves through the use of connectives or transitional words and phrases; adequate development -- the subject matter of the paragraph -- involves the who, what, when, where, and why, whether accomplished through definition, comparisons and contrasts, cause and effect logic, or analysis and classification; and, tone deals with not what the writer says, but how he says it.

BOOKBREAKING DIVISION

U.S. SECTION



That plain text doesn't make sense!
My recoveries must be bad again!

~~(C)~~ All four of these properties, we have insisted, are essential for good paragraph structure. But the one that usually causes lengthy discussions in class is TONE. We think this is good, because it tells us that the students are trying to be sensitive to "how it will sound" to the reader by steering away from unwanted tone. So they wrestle with another set of "don'ts": "Don't be offensive ... bossy ... contradictory ... and so on."

Managers: Are you with us?

In one of our classes in Expository Writing a discussion on paragraph tone developed after we explained how the tone of separate paragraphs in a piece of writing, say in a SIGINT report, ought to be consistent with the general tone of the writing. We gave the example of reports forwarded to the NSAPAC REP VIETNAM (NRV) staff in Saigon, in 1971, by one of the ten ARVN Special Technical Detachments (ASTD), which time and again reflected a tone of absolute terror. The perimeter of the site was not secure, and the ARVN people didn't seem to care. When the reports from this ASTD came in, the staff was obliged, not without some pangs of conscience, to change the tone of the reports to fit the dispassionate, objective tone of the monthly status report within which they were incorporated for forwarding to the Director (the Vietnamization Improvement and Modernization -- VIM -- report). One of the students, who obviously had after-the-fact sympathy for the plight of the writers of those reports (U.S. soldiers assigned to the ASTD), questioned the changing of the tone.

After we explained some of the unpleasant realities of the situation (we also apprised her of her handicap as a caring human being), she conceded that the tone of that ASTD's reports had to be changed and that our point on consistent and appropriate paragraph tone was well taken in the class.

Gobbledygook (U)

(U) We have described to your people in considerable detail the perennial enemy of good writing, namely gobbledygook or federalese -- the old obscure writing that is usually meant to impress rather than to express. We have convinced them (we hope)

- (1) that it is foolish to use high-sounding words, such as utilize, implement, initiate, viable, optimum, and terminate;
 - (2) that roundabout expressions, such as "It is believed..." and "There is/are..." make for weak writing because they tend to repeat, they are often vague, and they leave the reader with no way of knowing what is meant, thus forcing him to work for nothing;
 - (3) that we condemn the use of the expression "It is felt that..." because it has three inherent strikes against it -- it is roundabout, it is passive, and it is false (one doesn't feel an argument or a contention; one thinks it or one believes it);
 - (4) that circumlocutions, such as "Owing to the fact that...", "Concerning the matter of...", and "In reference to..." are nothing more than deadwood; and
 - (5) that illogical, incongruous, or inappropriate metaphors should be avoided.
- After analyzing the following real-world statements, we couldn't come up with a reasonably good answer to the question, "What happened to the quality control system?"

"The state of the art, as it exists today...."

"It's a sad day of affairs...."

"(We should be) starting out with a clean foot." (Let's call this one a combined, instead of a mixed, metaphor.)

Those gems are not any worse (or, if you like, any better) than the golden-oldies that were taken from letters received at a welfare department in Tennessee some years back (you old-timers might remember them):

"I am very much annoyed to find you have branded my son illiterate. This is a dirty lie as I was married a week before he was born"; "Unless I get my husband's money pretty soon, I will be forced to live an immortal life"; and "I am glad to report that my husband who is missing is dead."

(S) We shudder to think of what would have happened to our credibility in October 1962 if the [redacted] reporting staff [redacted] had gobbledygooked those FLASH messages they fired to NSA containing the first SIGINT reports on the Soviet merchant ships stopping dead in the water at the peak of the Cuban Missile Crisis. We also shudder to think of the possible unthinkable consequences of gobbledygooked guidance (from NSA) and gobbledygooked responses (from field elements) on matters about current developments in the world in general and in Eastern Europe and the Middle East in particular. The solution to NSA Crostic No. 35 (CRYPTOLOG, October 1981) contains a poignant comment from [redacted] Plain English that aptly supports all that we've been trying to say here.

If we want all Agency personnel to speak and write plain English, perhaps we should first teach Agency personnel English. If we want Agency management to write concise, active, decisive memos, perhaps we should first teach Agency management to be concise, active, and decisive. Let us attack the problem, not just the symptom.

(U) Having stated our case, we fully intend to continue to orchestrate drum rolls and trumpet blares for the cause of getting managers to cooperate in making clear, simple, direct, brief, and appropriate writing happen at NSA.

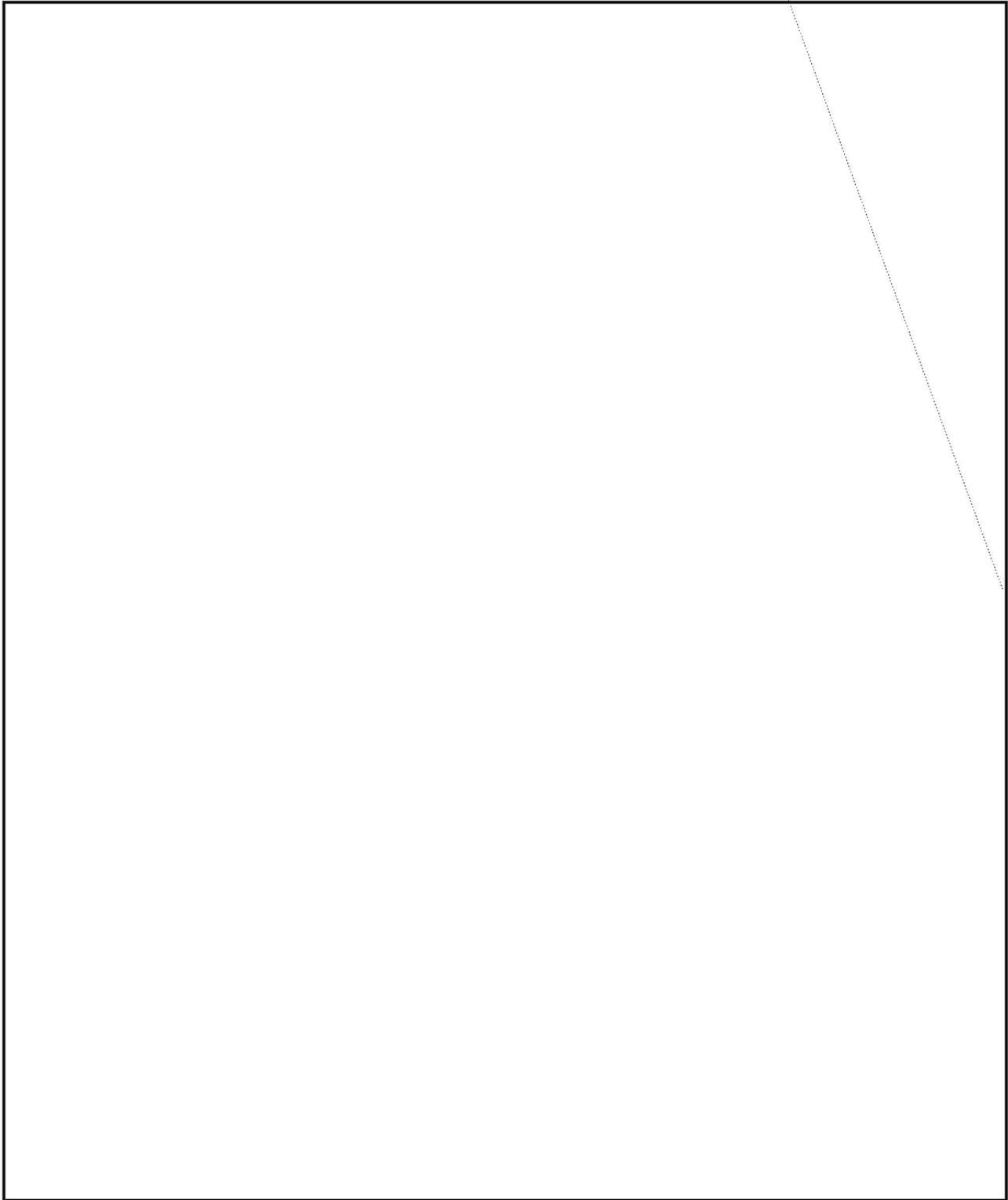
(1) Gobbledygook Has Gotta Go; U.S. Department of the Interior, Bureau of Land Management, p7. U.S. Government Printing Office: 1978 0-269-955.



~~SECRET~~

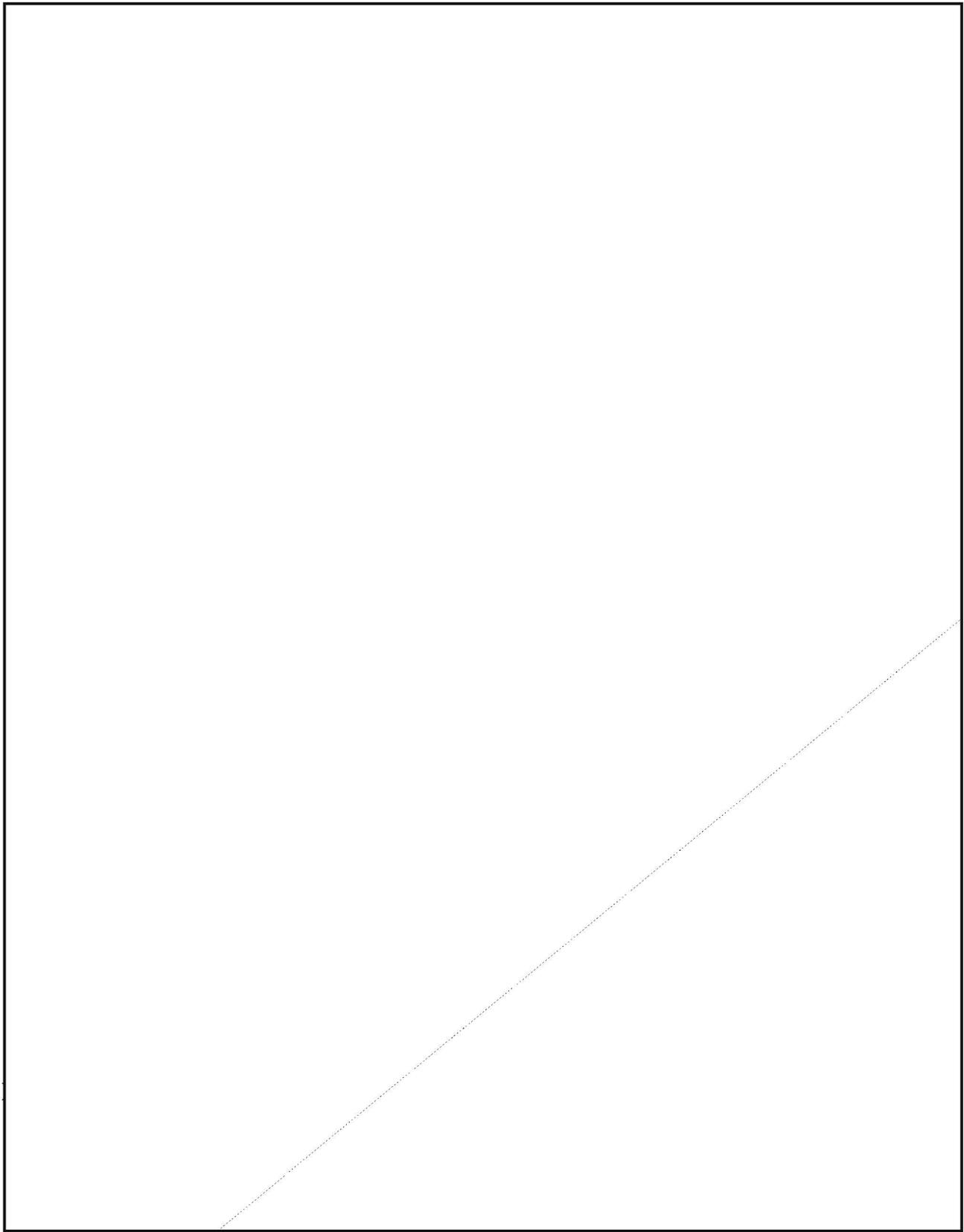
All The Alligators Aren't
On Sport Shirts (u)

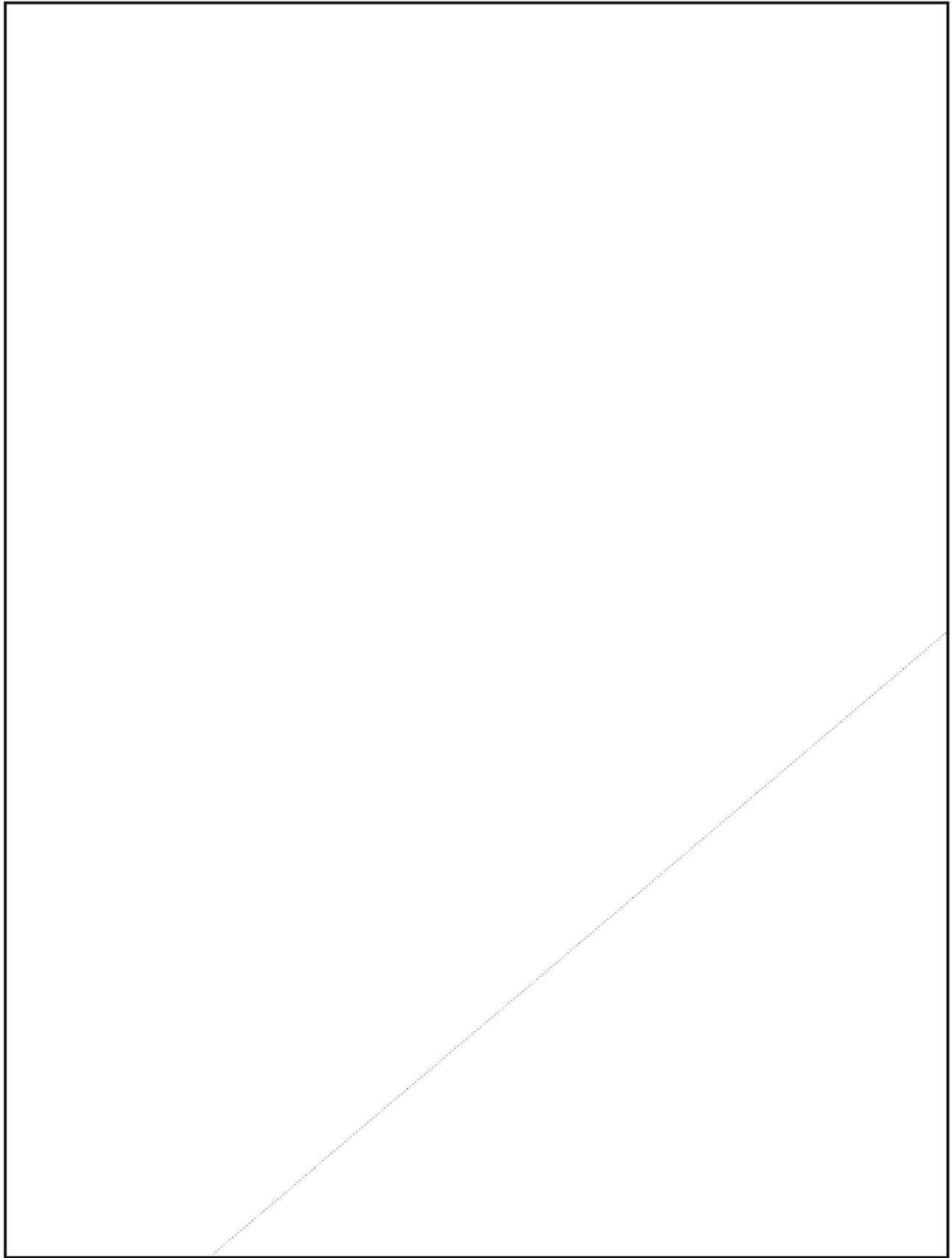
EO 1.4.(c)
P.L. 86-36



~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~





HUMAN FACTORS CORNER (v)

with P13

P.L. 86-36

REVIEW: "Information Systems - The Management Challenge", Joe Brancatelli, "Review" (Magazine of Eastern Airlines), October, 1981, p. 53.

Denny Eshoo, T441, kindly sent me this interesting article on a timely topic. In spite of its very general title, it specifically concerns the "Automated Office" or "Office of the Future" concepts being marketed by a number of firms. There are plans to introduce some form of "office automation" into NSA in the near future, for example in R. This paper provides a good overview of the concepts and some of the human factors problems already encountered by organizations attempting to jump on the office automation bandwagon today.

"Office equipment salesmen can't agree on what to call it, design professionals all give a different picture of it, visionaries see it coming, engineers say it's here, and some office workers want no part of it, ever."

Conversion of old-style offices to meet the new concepts will require a substantial investment. One estimate predicts that capital investment per office worker will increase from a current \$3000 a year to \$15,000 in 1990. And yet, according to this article, all the "experts" seem to agree that the sooner it happens, the better. They appear convinced that the expected gains will more than offset the expense.

The article does not spell out the real motivations that underlie the push for office automation. In fact, I cannot think of any place where I have seen them stated clearly, other than the usual vague words about "increasing productivity". However, reading between the lines, I think the following are prominent considerations: 1) White collar workers are increasingly numerous, and increasingly expensive, and automated "executive workstations" used by managers or staff

people could replace many clerks and clerk-typists; 2) Office procedures involving communication, coordination, and records-keeping are becoming increasingly burdensome and difficult to control. This is blamed primarily on "too much paper" ("paper is the nemesis of the modern office"), though I can see some possibly more basic reasons for the problem; 3) Travel is becoming increasingly expensive, and electronic conferencing could effect a saving in time and money; 4) Managers perceive an increasing problem in getting and keeping a good "handle" on what is going on in their organization. This is blamed on "the paper problem", but is probably a more basic problem of fragmentation of effort and poor communication, exacerbated by the understandable reluctance of subordinate managers to relinquish any control over THEIR records to others. Automated, "paperless" distributed information networks might help solve this problem, if well designed to solve the real difficulties and not just to "abolish paper". In short, the automated office offers the manager a vision of a paradise in which he holds a smaller number of much shorter reins controlling all corners of his enterprise.

The early expectations of rapid changeover to automation in offices have run into some roadblocks.

"Current wisdom, based on the experience of the past two decades, indicates that the office of the future will evolve slowly and methodically over the next twenty years."

The crucial problem seems to be resistance from some "tradition-bound managers and professionals".

"You can't forget that office automation is introducing significant amounts of unfamiliar technology into a world where a great many people still hang up when they get a telephone answering machine . . . All the managers in an office have reached their current level of responsibility by using a set of communication tools they and everyone else understand . . . Suddenly, someone says, 'Forget all that, here's a new way to do



things with keyboards and video screens and electronics.' That's a scary transition to make after decades of hard-copy files and telephone messages."

There is another obstacle between managers and the "executive workstation", and one that may not be restricted to those who are older or more traditional. If the intent of the automated office is to replace the manager's secretary with a workstation operated by the manager himself, we will run up against a key element in "corporate culture" that cannot be ignored.

"Managers and professionals . . . routinely delegate clerical tasks to secretaries and other support personnel. Most of these clerical tasks involve typing, a skill managers on the whole do not value highly . . . and until more advanced methods of access become feasible . . . managers and professionals alike will be asked to operate their workstations by typing messages on a keyboard". One expert says, "I know middle-level managers who have been told not to punch information into a word processor because it doesn't look right . . . Managers view any kind of typing as a menial task. They say to themselves, 'I shouldn't be doing this.'"

Another, even stronger barrier relates to the status that a real, live human secretary confers on the manager. Along with the private office, comfortable furniture, and picture window on an upper floor, a secretary is one of the major perks of being a manager.

"Losing a secretary, office-automation experts now realize, isn't just losing support personnel. In the pecking order, a secretary is also a tangible symbol of the manager's importance."

Thus, the hope of replacing expensive humans with supposedly less-expensive machines may have to be set aside, at least when it comes to the secretary in the front office (though the typing pool may not be so fortunate).

Perhaps the best hope lies in making "executive workstations" into a new kind of status symbol (e.g., giving one to the President first, then the VP's, and so forth), and in making them as different as possible from typewriters! I am afraid that the thought occurs to me that one of the reasons why typing and typewriters have such a "menial" image

for managers is that they have traditionally been operated by women. Maybe the solution lies in putting the "executive workstation" in a "macho" package: making it look a lot like a control station for space missions, or the console of a nuclear power plant, and providing large banks of "menu" buttons for sending pre-programmed commands! That might enhance the manager's feeling of finger-tip control, god-like power, and remoteness from the squalid associations of keying in text.

The Xerox STAR is the first step toward developing an "executive workstation". It handles word processing, electronic mail, electronic filing, some rudimentary computing, and some other functions. While it has a keyboard, many of its functions are controlled by touching "icons" (symbolic pictures) with a simple hand movement, rather than by typing in commands. There are icons for activating the filing system (a file folder), documents, file drawers, in- and out-baskets, and printers. While not the last word by any means, the STAR "goes much farther than any other product on the market". Unfortunately, the workstation is useless alone, without a local network tying it to other stations, printers, filing devices, etc.

"Networking technology is progressing rapidly, but strong marketing competition between exclusive systems may actually be slowing advancement. At least six major vendors are peddling non-compatible networking schemes."

In any case, it seems best to start small, to carry out the automation process slowly and carefully, and to make it as voluntary as possible. Seven to ten years may be needed to make the switch complete in any given organization. "What we're asking people to do is change how they function, and that's not easy. We've found that people come around to office automation individually. But they come around at their own pace, and you can't rush them." Here are some "Tips for Transition" offered by the writer of this article:

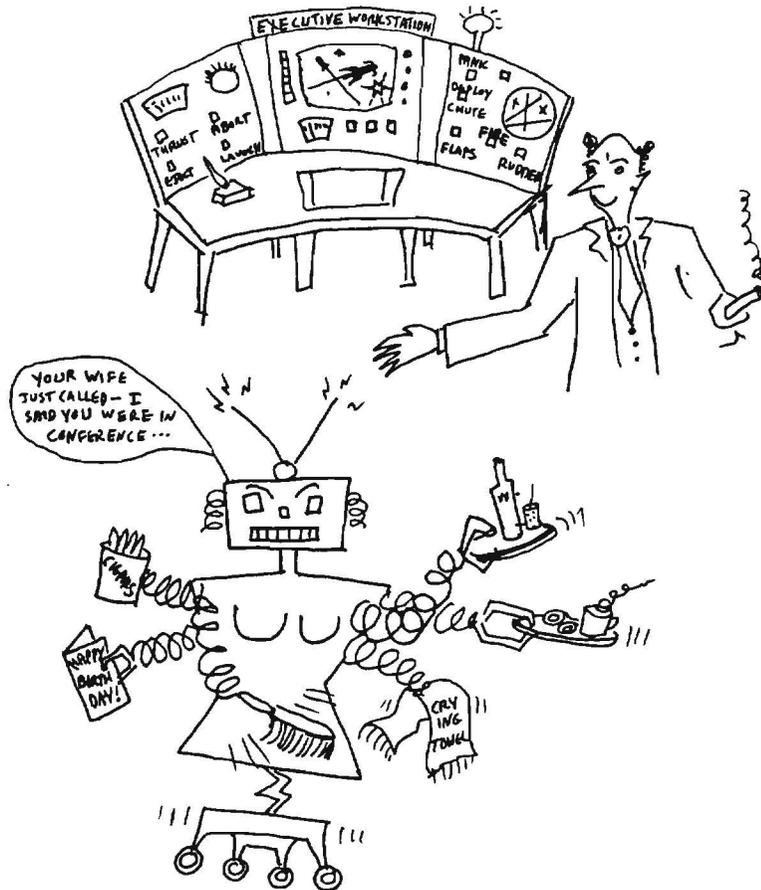
"Start small. Introduce new technology on a department-by-department basis. Don't overwhelm employees with a vast, company-wide change. Proceed gradually. Phase in new automated systems and services rather than introducing them all in one indigestible lump. Introduce

office automation technology only into those areas where benefits are immediately needed and will be immediately evident. Integrate the new technology into your existing system and office structure. Present new equipment and services as aids to increased productivity, not replacements for secretaries and support staff. Select an automated system that is compatible with the needs and preferences of your employees. Consult the potential users of the new technology before you start. Let them have a say in the system they will be using. Provide heavy and continuous training in the use of the new products and system both during and after the introductory phase. Integrate new equipment into the 'corporate culture' as one of the trappings of executive power. Managers will want an executive workstation more if it is a benefit awarded as a symbol of success.

sionals are using the new equipment, resisters will fall in line as they realize that their refusal places them at a disadvantage. Allow each person to adjust to the new system at his or her own pace. You can't rush the learning process. Be prepared to wait out a possible 'generation gap' between older and longer-tenured managers, who are more likely to resist the change, and younger or newer ones. If possible, target the latter group for the earliest transition, since it is usually more familiar with automated equipment and more flexible or more eager for the change. Start immediately. Moving into the automated office of the future takes time for phasing in and adjustment."

"Don't force anyone to use equipment he or she doesn't want to use. If the majority of your managers and profes-

The above "Tips" hold good for any introduction of new technology, and are by no means restricted to office automation. We ignore them at our peril, especially when we consider automating some of our work areas which are still entirely oriented toward the traditional tools: typewriters, paper and pens.





*Letters
to the Editor*

Ref: Persephone
Terpsichore (April-June 81)

Webster's Second Unabridged has adequate descriptions of these Greek mythical personae.

Terpsichore (as illustrated by you) was associated with the dance and was not strictly a goddess but a lesser person (nymph).

Persephone was a daughter of Zeus and wife of Pluto, ruler of infernal regions (Hades) and presumably not much given to gaiety (dancing).

It is 1000 to 1 that you know all this already and just stuck the item in to see if there would be any reader response!!



P.S. I was bemused to find that according to [redacted] NSA has at least one employee capable of making such a statement as "nonferrous steel is steel without any iron in it."

R.C.

Dear Joe,

Just read your excellent piece on The Stairwell Society in CRYPTOLOG (October 81). It's high time someone publicized this important activity.

Several people who have been trapped repeatedly in the elevators in the International Tower Building have asked about the possibility of forming a FANX/ITB chapter. Minor league, of course, since the buildings

out this way are only seven stories high.

If the interest in stairwell climbing continues to grow, the National Cryptologic School will present two new training courses in its stair climbing curriculum: SC-101, Avoiding The (elevator) Shaft, and SC-301, Up Your Staircase.

Inasmuch as secret societies inevitably attract the attention of the lunatic fringe, the possibility exists that Philip Agee may publish the names of the secret Society members in his Covert Action Information Bulletin, after he finishes with the other secret society he writes about.

You might also consider adopting a cheer or motto for your Society, something along the lines of --

Up on the riser,
Over the tread,
Too wide a Bloom arc
And you land on your head.

As they say on the buses, Watch Your Step.

Ed Wiley

P.L. 86-36

Cryptanalysis articles have been hard to come by in the past, although I believe there are a wealth of interesting articles out there, particularly in the hand systems areas.

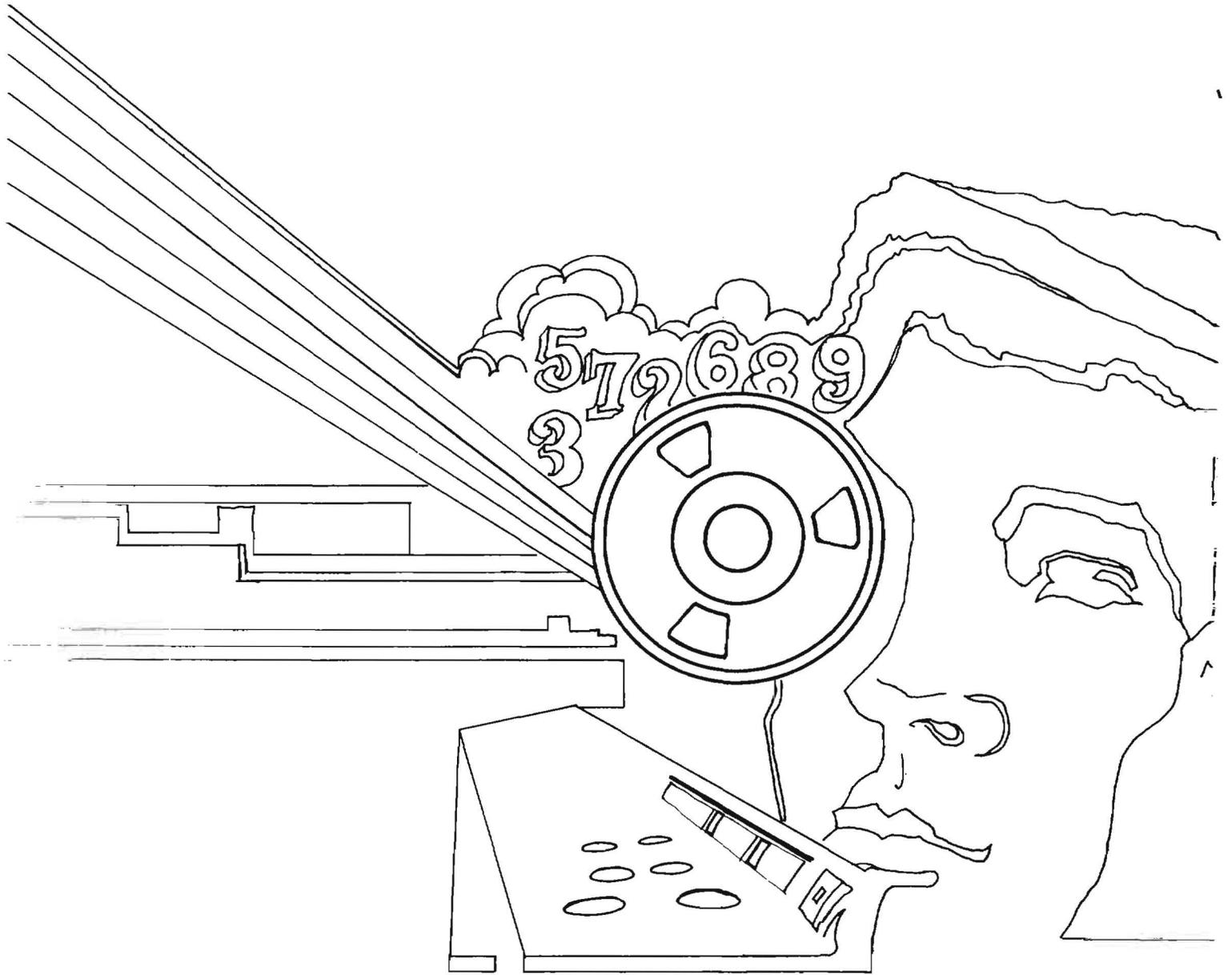
We need some incentives for short articles. How about a "Strangest Bust of the Month" contest?



SOLUTION TO NSA-CROSTIC No. 36

["A Traffic Analyst Looks at] Computers,"
[redacted] CRYPTOLOG, Apr-Jun
1980

". . . contrary to popular [view], we analysts were not afraid of computers. Maybe some [of us] were, but not all. But what we all did share was the realization that our processing cycle was no longer solely under our control. Our data was in a loop that went through someone else's area of control."



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~