

~~SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

JUNE-JULY 1982



P.L. 86-36

P.L. 86-36

WHO WANTS A PROMOTION, ANYWAY? (U).....	[REDACTED]	1
AMATEUR SPREAD SPECTRUM (U).....	[REDACTED]	6
REPORTING MESSAGE VOLUMES (U).....	[REDACTED]	10
A PERSONAL FOOTNOTE (U).....	[REDACTED]	17
NSA-CROSTIC NO. 41 (U).....	David H. Williams	18
RESPONSIBLE DOCUMENTATION (U).....	[REDACTED]	20
SOME REFLECTIONS ON THE.....		
REALITY OF COMPUTER SECURITY (U).....	Robert J. Hanyok	23
ODDS AND ENDS (U).....		25
MAILBOX (U).....		26
A LOOOONG SHELL (U).....	[REDACTED]	27

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~

~~CLASSIFIED BY NSA/CSSM 123-2~~
~~REVIEW ON 10 Jul 2012~~

CRYPTOLOG

Published by PL, Techniques and Standards

Editorial

VOL. IX, No. 6-7

JUNE-JULY 1982

PUBLISHER

BOARD OF EDITORS

Editor-in-Chief. [redacted] (8322/7119s)
 Production..... [redacted] (3369s)
 Collection..... [redacted] (8555s)
 Cryptanalysis..... [redacted] (5311s)
 Cryptolinguistics..... [redacted] (1103s)
 Information Science. [redacted] (5711s)
 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)

For subscriptions
 send name and organization
 to: CRYPTOLOG, PL
 or call [redacted] 3369s

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

P.L. 86-36

~~(FOUO)~~ The other day, one of our regular contributors got us all laughing about an idea he had: put advertising into CRYPTOLOG. Lots of contractors, he said, would be willing to pay for advertising space in a technical magazine that went to almost all of what we call the "technical underside" of the Agency (apologies to Churchill). He thought we could make enough to pay for the publication costs and maybe my salary too.

~~(FOUO)~~ After a while, the enormity of the possibilities began to come to our minds. When you put a query into a terminal and then wait, staring blankly at the unchanging screen: why waste all that space and time? Why not a quick message from a contractor or company (selling a faster system, perhaps) to redeem the time? Did you ever get a computer print with all that blank paper in front and back? Why waste the paper? Let the kids doodle on something else; put some advertising there, and help pay for your output!

~~(FOUO)~~ Why, we could sell space in the Green Hornet! Think of all those blank walls all over the building; let the advertisers pay for the paint! And the public address system--why not get sponsors for each announcement? We could stipulate that the sponsor's message could only come after the emergency messages, of course. And for those big meetings in the auditorium, some advertising on the screen might keep the audience from getting restless until the main speaker arrives.

~~(FOUO)~~ The end walls on the outside of the tower are just huge blank spaces; does anyone know if Mail Pouch still paints barns? Too bad Burma Shave doesn't still do those sequential signs, considering all the roads and parking lots we have. The bus that runs between buildings, the elevators, the escalators, the cafeteria walls--the opportunities are everywhere. We might finish the year showing a profit! The possibilities just boggle one!

WES

WHO WANTS A PROMOTION, ANYWAY? (w)

by T1
Col, USAF



P.L. 86-36

When I was asked to address you, I pondered what would be the best subject to share with you. I thought I could talk about state of the art (FOUO) technology--computers, distributed processing, digital systems, fiber optics, millimeter radios, wired cities, and the like, but I decided that you have been force-fed Communications-Electronics long enough. Then I thought I would tell you about my job.

Our computer operations is one of the largest, if not the largest, as is our production signals processing effort. For you country folks, the area of responsibility is more than seven acres, and for you city people, that's about 30 city lots or homes. Isn't that impressive? Sure, it is! But that isn't going to help you in your Air Force career; so that's all I'm going to say about my job.

I have an additional duty that I consider most important to the individuals with whom I talk. About two years ago, General Larson, the Commander of the Electronic Security Command, was concerned that his people were not getting as many promotions as he thought they should. He established an Officer Career Development Panel consisting of 12 Colonels around the world to counsel each officer (O-5 and below) at least once a year. I am one of those Colonels and the duty can be rewarding--

Some of our readers are Air Force officers, and others are or will be supervisors or coworkers of Air Force officers. Both groups should be interested in these remarks, adapted from an address by USAF, to the Communications-Electronic Officers' Course at Keesler AFB, Mississippi, on November 1981.

It can also be discouraging. We meet "two on one" to review the officer's records as a promotion board would. That is what I wish to share with you today--what promotion boards look for and what you need to do at what point in your career to be competitive for promotion.

Ladies and Gentlemen, your promotion folder is all the board has to represent you! The accuracy and completeness of the data in that folder is your responsibility--no one else's!

Let's review it! The first thing we see when we open the folder is your official photograph. You've made your first impression on the board members. Whether that is good or bad depends on your picture. That picture can say, "Hey! I'm out here and I want to be promoted!" Or it can say, "Eh. Take me as I am! Promote me or don't; I really don't care!" Surprised? Don't be! There are records that say just that; and when the officer gets passed over, he or she says, "Why me?" If the photo isn't the best, the rest of the record probably isn't either.

~~FOR OFFICIAL USE ONLY~~

Let me share an experience with you. I think it was on my first promotion board. One of my panel members opened a folder, made a disgruntled remark, and immediately laid the folder aside. Why? He didn't like the length of the officer's sideburns. They were regulation length but only a hair's width from becoming too long. That was enough to turn that panel member off on that record. Petty? Maybe so! But competition is keen and when records are nearly identical, board members find themselves looking for "tie breakers," and those tie breakers go for or against you.

Let's prepare for your photo. Gentlemen, the day you have your picture taken, or the day before, get a haircut. Ladies, have your hair done or do it yourself. Have your photo taken early in the morning. At the Pentagon, they won't take it after 1000 hours because they have found that "the five o'clock shadow" shows by then. Insure that your sideburns are squarely cut and short. If I had a mustache, I'd shave that hummer off for the photo; there are just too many things you can find wrong with a mustache: too thick, too thin, too wide, too long, too short, not trimmed. You name it; they'll find it.

The most common discrepancy on the photo is that the U.S. insignia are improperly aligned. The letters must be positioned horizontally (parallel with the ground), halfway up the lapel seam, resting on it but not over it; and they shouldn't be tarnished or polished to a high luster. You get into your sharpest uniform (one without a near-term wearout date), stand in front of a mirror, position your U.S. insignia, center your rank on the epaulet 5/8" in from the outer seam, center your name tag and your neat, correctly sequenced ribbons with the devices properly placed so they are resting squarely on top of your pockets but not covered by your lapel, and you're ready for the photographer. Right? Wrong! Why?



Because your photo is taken sitting down and when you sit, everything gets "out of whack." When you set your uniform up, sit in front of the mirror, the way you will sit in front of the camera. To have you uniform hang neatly, you may need to open the bottom button of the jacket, and that's OK. The picture will be cropped, so it will not show. Just don't forget to button it before you leave the studio.

That's a lot about the photo: but, as they say, first impressions are lasting and, at an average time of three minutes per record, you don't have long to change that initial impression. We women don't have the pockets to help us line up our name tags and ribbons. The important thing is to have them parallel with the ground and at the same level.

When you come up for promotion consideration, get a new picture. An old picture doesn't tell the board that you want to be promoted. Make that little extra effort. It's impressive when you see a photo taken last month.

One other thing, gentlemen: snug up that tie. A loose tie, especially with your shirt showing above it, makes a negative impact. The same for the ladies! Your blouse should not show above your tie. Enough about the photo.

Your OERs have to be great or you don't have a fighting chance. That's not to say that you can't get promoted with a "2" or "3" if you got them during the controlled OER period. If your rater tells you today that he's giving you a "2" to "give you room to improve," you'd best talk turkey to that turkey. A "2" today says you're in the bottom five percent of your peer group.

Your OERs are a record of your past performance and an indication of your potential. They tell when and where you did what and how. They should have facts in them. When I gave you that 30 seconds on my job, it had several facts in it, and that's what the narrative in the Job Description block of your OER should contain. The same is true for the Performance Factors blocks and the three Comments blocks. You can have a "fire-walled" OER with a "1" rating, but if the comments and remarks are all general, it tells the board nothing; or maybe it says, "we've got better people. He or she is OK but ...!" The board looks for substantial accomplishments and recommendations for promotion. "Promote when eligible" doesn't say much: eligible for what? Below

~~FOR OFFICIAL USE ONLY~~

the zone? Primary zone? What? They look for

- "Promote now"
- "Promote BTZ" (below the zone)
- "Promote first time eligible in the primary zone"

They look for good endorsements and general officer endorsements carry a lot of weight, especially if it is obvious that the OER was elevated for a high level endorsement in the chain of command.

Your selection folder contains citations for approved decorations. If your photo shows a ribbon, wings, missile badge, or any device not supported by a citation, order, or other documents, it looks suspect. Among the miscellaneous documents are administrative requests to obtain missing documents. Often we find these requests stamped with "second request." It is to your advantage to provide the missing documents or current photo as soon as you receive the request. No one can do that for you. I hope that you have a complete personal 201 file and can retrieve the required documents with little problem.

The next form is not in all folders and many of you have never heard of it. AF Form 11, the Officer Military Record, is now a historical document that was last updated in 1974. Your Form 11, if you had one, remains part of your folder.

Next is the Officer Selection Brief, a computer generated form that contains a wealth of information about you. About 60 to 90 days before a board convenes, each eligible officer receives his or her Officer Preselection Brief through the servicing CBPO. This Preselection Brief contains the same information as the Officer Selection Brief that is part of the folder evaluated by the board members. You are responsible for reviewing the Preselection Brief and having any errors or omissions corrected by your servicing CBPO. I won't cover all the data elements in the Brief, but I do want to cover a few in some detail: the most frequently problem areas.

Let's start with formal education. Almost every officer has a bachelor's degree; very, very few do not. I don't have the exact figure, but the percentage of Captains and above with master's degrees is in the high 90s; the degrees are not all job related, but they are master's degrees. There are several avenues you can take to get an advanced degree. Check

out AFM 36-19. You can go AFIT, BOOTSTRAP, Naval Post-Graduate School, and on- or off-base/campus programs. If you want an AFIT program, don't wait for AFIT or a selection board to pick you up: request an AFIT evaluation. They will evaluate your records and tell you whether you are qualified, and you could find yourself in one of their programs before you know it. It's not commonly known, but there are AFIT slots that go unfilled every year. Just don't wait until you come up for Captain before you decide to start working on your master's. It's too late then! Do it! Get it on your record! And, if possible, apply the degree knowledge to your job.

Another shortcoming often seen is in the area of Professional Military Education (PME). I don't know if the officers are waiting to be picked up by a selection board to attend in residence or what. I do know that PME is often missing in an otherwise good record. I know it's tough to complete your degree requirements and PME by correspondence, especially if you have a family. The youngsters don't always cooperate when it's time to concentrate and study. Everyone cannot be selected for PME in residence; maybe 38 percent get to go, so don't wait for it. Complete the correspondence courses and if your name comes up for residence, so much the better. Go if you can, but don't count on it. You may be selected and denied the opportunity to attend because of operational requirements. Again, don't wait! Get cracking on your PME. Time goes by all too fast and if you put it off, it will soon be too late, and your records will not be competitive.



~~FOR OFFICIAL USE ONLY~~

There is controversy regarding completing PME in residence or by correspondence. Some believe that the "cream of the crop" are selected for residence, and it's true that the interaction and exchange of ideas between officers in residence add value to the PME course. It's also true that those experiences are available on on-base seminars, and if pure correspondence courses are difficult for you, join a seminar. If there is no seminar, consider starting one. That's super OER material! Others believe that completing PME by correspondence show a greater drive and initiative in the officer. He or she performs full time duty for the Air Force and still gets the PME; in residence, the officer is a full time student, not directly contributing to the mission during that time. There are advantages and disadvantages to both methods. Just do it, one or both ways, and get it into your records.

The time requirements change to register for PME correspondence courses, but generally speaking, Lieutenants should complete Squadron Officer School; Captains and Majors should get an intermediate Service School (Air Command and Staff, for example; some officers take the Marine Command and Staff while they wait for the "time in service" requirement to take Air Command and Staff), and Majors and Lieutenant Colonels need to get a Senior Service School: Air War College or Industrial College of the Armed Forces, or both.

One other thing about PME: your file may contain a PME letter telling the board

- that you declined to attend residence PME courses for personal reasons, or
- that after being selected for attendance, you were denied the opportunity to go because of operational requirements.

Other data elements in your brief include your date and source of commission, the date you came on active duty, dates of promotions, dates of and levels of assignments, overseas dates, rated information, awards and decorations, distinguished graduate information, and a few other data elements.

Awards and decorations are often a function of being in the right place at the right time, or the wrong place, as the case may be. If you don't have many, or any, don't worry about them. There isn't much you can do except hope that your supervisor is a someone that will take the time and effort to write the recommendation that documents your outstanding

performance--assuming it was outstanding, that is. It isn't easy! It takes someone's time and effort to write a good recommendation for the awards board's approval. Our Director can approve the Joint Service Commendation Medal and the Defense Meritorious Service Medal; anything higher must be sent outside the agency for final approval. It gets frustrating and I can understand the reluctance of some people to write recommendations for decorations; I guess you could help your supervisor by given him some notes or even drafting the recommendation. Some supervisors would appreciate that. Others wouldn't process the recommendation anyway, so you need to be tactful and know your supervisor well before suggesting either approach.

Some folders have unfavorable information in them. I hope you won't have any of these documents in your folder, but if you earned them, they will be there. Correspondence reflecting an Article 15 or Court Martial remains in your folder for two years or until reviewed by one temporary or permanent promotion board, whichever comes first.

Also undesirable in your folder is what's called "not qualified recommendation or digest file." These are forms of derogatory data that have been reviewed through command and legal channels. The officer involved is notified in writing of the existence of these files and has appeal rights. What can I say about these types of correspondence? You don't want them; don't do anything to get them!

Next comes the AF Form 705, Lieutenant Colonel Promotion Recommendation Report. This report is used only by Central Temporary Colonel Boards. These forms were written on Lieutenant Colonel OERs that closed out on or before 30 June 1981. No 705s are written on officers for a reporting period after that date, but all 705s previously submitted remain a matter of record in the selection folder.

One other piece of correspondence may be found in the selection folder. Since DOPMA, an eligible officer may write to the board, calling attention to any matter of record that he or she believes is important to his or her consideration. A couple of words are required on that. First, decide seriously whether you want to address the board about your record. If, after careful consideration, you decide to write a letter to the board, make it factual and to the point. Do not, and I say again, do not be emotional and do not blame anyone else. Accept responsibility for your action or lack

~~FOR OFFICIAL USE ONLY~~

~~FOR OFFICIAL USE ONLY~~

of action. If you were a victim of circumstance, you can say that--but be factual about it.

So much for what the promotion board panel members look at and for. I'd be remiss if I failed to tell you that you may review your selection folder at the Air Force Manpower and Personnel Center (AFMPC) at Randolph AFB, Texas. If the folder is incomplete or contains incorrect information, take immediate action to have it corrected or completed.

Having said all that, just what is the purpose of promotion boards, and what are your promotion opportunities?

Well, promotion boards insure that enough officers of the desired quality are in the proper grade to carry out the Air Force mission. Promotions should occur at spaced intervals to insure that the best qualified officers are promoted to positions of authority and responsibility. A promotion is not an award for past service; it is an advancement to a position of responsibility, based on past performance and future potential.

Your promotion opportunity is determined by the percentage of each year group that can reasonably expect to be promoted to the next grade, and that is determined by Air Force requirements. The quota is an established percentage of those officers "in the promotion zone," that is, the first time eligibles (new eligibles):

- 97.5% to Captain
- 90% to Major
- 75% to Lt. Colonel
- 55% to Colonel

These percentages are misleading, because those selected "below the zone" and "above the zone" (those previously considered but not selected) are at the expense of the new eligibles. Considering that, your opportunities are reduced considerably:

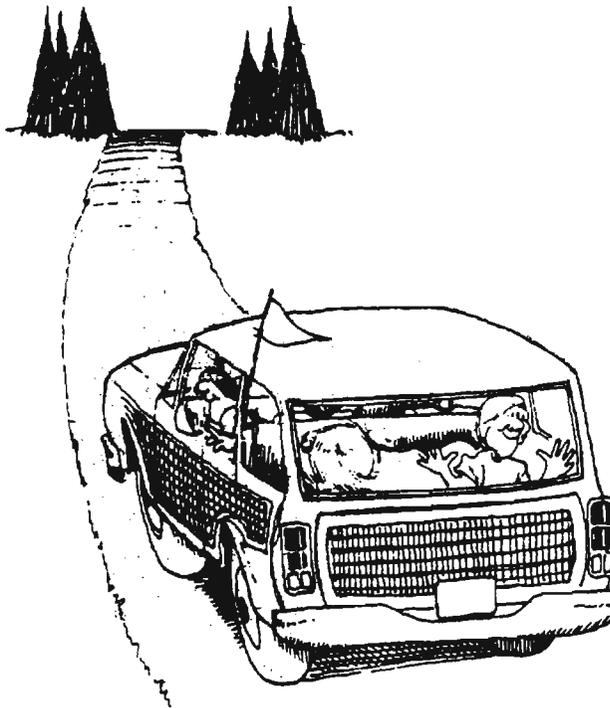
- from 90% to 75% going to Major
- from 75% to 60% going to Lt. Colonel
- from 55% to 35% going to Colonel

An earlier study showed that only six percent of all newly commissioned officers make it to the Colonel level. Of course, many resign their commissions or retire before they become eligible for Colonel; still, six percent isn't very high.

I wanted to mention some factors that would help you get those good OERs I talked about earlier: being flexible, making frequent moves, getting into all facets of Communications-Electronics (Operations, Maintenance, Programming, Budgeting, and don't let computers scare you), relying on and respecting your NCOs and airmen, seeking challenging jobs, and a thousand other things. If you don't know about the ASTRA program (Air Staff Training Program), find out about it. It's tough, but if you want to go far and fast in the Air Force, apply for one of those positions, be successful there, find a General Officer to sponsor you, and you'll get "below the zone" promotions and super jobs.

I realize that I've shared a lot of material with you in a short time. I trust you will find it useful in your career.

Now, I know that the graduates have everything they own in the car, including the dog and the cat, and some of them even have the engine running, so just let me extend my best wishes to each of you for a long and successful Air Force career.

~~FOR OFFICIAL USE ONLY~~



AMATEUR SPREAD SPECTRUM(U)

P.L. 86-36



(U)

Amateur Spread Spectrum communications appear to be in the doldrums, according to Paul Rinaldo, President of AMRAD, a Ham corporation that has been investigating this new mode.

(U) The central problem is that there is no market for spread spectrum communications either among Amateurs or among other civil users. The comments received by the FCC have been mostly against spread spectrum, because of potential interference problems. AMRAD Corporation got an STA (Special Temporary Authorization) in 1981 to waive cipher and bandwidth and other restrictions in order to experiment with frequency hopping and direct sequence coding transmissions, but only a few experiments have been carried out. AMRAD will ask for a new STA to try again in 1982-83, but the combination of apathy and indifference by the Amateur community does not show much promise. One new equipment was developed, viz., a 2 meter frequency hopping radio, by an amateur who hoped for foreign sales. His equipment apparently worked, and he found customers.

(U) Rinaldo summed up the AMRAD experience of the last year at an IEEE-VTS meeting on 28 May 82, and a current report in the AMRAD Newsletter reinforced many of his points. Amateur packet radio is apparently doing quite well, and spreading, but spread spectrum is faltering, and the projects have failed to reach completion.

(U) In his opening remarks, Rinaldo noted that Spread Spectrum is "controversial." There are popular beliefs that Amateurs "can't receive it," or if they could receive it, could not decode it. It is also believed that Spread Spectrum cannot be "DF'd," and hence cannot be monitored. Therefore, according to Rinaldo, there is popular belief that it is open to abuse by spies, criminals or terrorists. It is also popularly believed that the spread signals would interfere with everything, like the "Russian woodpecker" at 14 MHz that interferes with HF communication. It is also popularly believed that narrow band communications can do the same thing.

(U) These popular beliefs, Rinaldo said, gave a distorted picture of Spread Spectrum. He said he had been using SS for years.

(U) The starting point for Amateur involvement in SS communications, which was previously only a military technology, occurred when Dr. Marcus of the FCC OST (Office of Science and Technology) approached Perry Williams of the ARRL (Amateur Radio Relay League) and asked ARRL to push the development of Amateur SS. The purpose of this FCC initiative was to get cheap SS equipment onto the market. Since Amateurs were known to be adept at finding cheap ways to put radio gadgets together, the FCC apparently hopes the Ham community could do what the U.S. military electronics industry could not do, viz., develop low cost SS

~~CONFIDENTIAL~~

radios, which the FCC could then authorize for use in many different radio services where frequency crowding (e.g., in urban areas) was causing complaints to reach the FCC.

(The author has heard rumors that the FCC gave the impression that the Amateur frequency allocations could depend upon how well the Amateurs responded to this opportunity to develop SS. The issue of Amateur SS was so controversial to foreign governments that the ARRL had to adopt the euphemism "low flux density modulation" in their correspondence to avoid friction with the corresponding foreign Amateur associations).

ARRL then interested the AMRAD Corporation in spearheading this new project. AMRAD itself is a Ham club organized as a legal corporation (AMateur Research And Development), with about 600 members, some of whom apparently are foreign. Its newsletter is mailed to foreign and overseas subscribers. The aim of AMRAD is to pursue new technology projects (of which SS is one), and to disseminate technical information. A number of the people involved in the AMRAD SS experiments claim to have had experience with spread spectrum and cryptologic systems (for both encryption and interception-analysis). The AMRAD Corporation operates a repeater and a message system in the Washington area.

(U) The two experiments actually conducted under the STA were an HF frequency hop communication, using two RACAL S.A. transceivers imported by MILCOM, and a VHF 2 meter frequency hop experiment using equipment built by an Amateur who was interested in overseas sales. Rinaldo played an audio tape demonstrating the HF experiments between Kessler of MILCOM in Providence, R.I. and Rinaldo of AMRAD in Virginia. SSB voice and Morse code were both used, with hopping at 5/sec, after an initial setup, callup, and synchronization in a non-hopping mode. The VHF experiment in Virginia during February worked in the 150-174 MHz range. The experimenter, C. Phillips N4EZV, has now sold his VHF gear and intends to experiment in the 14 MHz and 21 MHz bands at speeds up to 80 hops/sec.

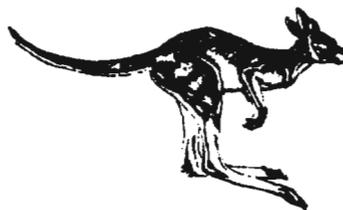
(U) The SSB HF experiment illustrated that frequency hopping doesn't work well on weekends, when the Ham bands are full, but during the week when there are empty frequency slots it is feasible.

(U) The proposed experiment at 10 meters,

which was to modify CB radios to frequency hop at 30 MHz, is not yet finished. AMRAD wants to get a new STA to pursue this. Rinaldo thought that the equipment for the modification would be inexpensive, if they could get the circuit to work, and get volume production of the circuit boards. (Note: a Ham packet radio circuit board sells for \$35). The 10 meter experiment has not yet gone on the air. The proposed experiments at 400 MHz, to use direct sequence coded signals through a repeater, have languished without any finished equipment. A 420 MHz experiment to do SS moon bounce, using the 85 meter government antenna at Cheltenham MD, has also languished.

(U) The demonstration of frequency hopping at 2 meters has raised a question about whether a hopping signal might activate a Ham repeater. Rinaldo thought the squelch circuits would suppress short random pulses that got into the repeater control channel.

(U) The FCC Docket 81-413, asking for comment on general Spread Spectrum use, received mostly negative comments. "Not on my frequency!" was the theme of the comments. Most of the comments did not take the near-far effects of SS into account. Rinaldo stated that the "near" effects, where a receiver listening for a weak signal is close to an SS transmitter, is much worse than people expect. Very few comments on FCC Docket 81-413 thought SS was a good idea. Rinaldo sounded somewhat discouraged by the resistance to this new technology.

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

(U) The FCC Docket 81-414, asking for comments on Amateur Spread Spectrum, received replies that paid lip service to "experimentation," but "not on my frequency!" There were fewer than six comments, and most were from Hams who wanted to receive weak signals and feared SS interference. AMRAD filed favorable comments to continue SS experiments. There appear to be no applications for SS, except for experiments. Rinaldo did not expect an operational SS service on the Amateur bands.

(U) The basic question in civil and Amateur use of SS is, what good is it? The technology is a military development, to give LPI (low probability of interception). Rinaldo said that it is now being revealed that SS signals can be detected, although it takes special apparatus. He did not say who was revealing this. Rinaldo thought there might be a use for SS for police surveillance, viz., "bumper beepers" that could be attached to some citizen's car and could not be detected by a conventional radio sweep. He also thought SS could be used to defeat police buffs, who monitor police radio traffic. (Presumably these would be frequency hopping radios, and the AMRAD Newsletter of May 1982 claims there is a concept for a receiving system that would not need the code sequence).

(U) The most promising ways of solving the near-far problem were to locate the radios or repeater in remote places, e.g., a satellite repeater, or offshore oil platforms. Since there are very few signals in remote locations, the SS systems cause fewer problems and work better. However, narrowband systems also work better in a sparse environment. Operating SS stations in the midst of a dense population of radios, e.g., in a city, will cause many problems, according to Rinaldo.

(U) Rinaldo concluded that SS was neither a panacea nor a nefarious plot. He felt there were some specific civil applications, although they would be rather specialized.

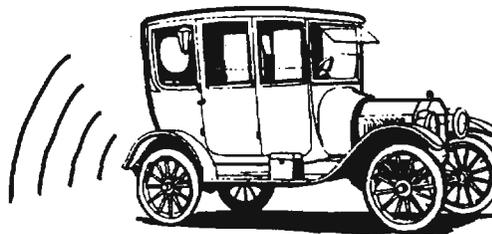
(U) Rinaldo then played a tape recording of the Kessler-Rinaldo HF SSB frequency hopping experiment. The voice transmission had many little clicks and bleeps, that changed every 200 milliseconds as the radio hopped. The Morse transmission also had a pattern of short changing bleeps. When the SSB voice channels are busy on weekends, there is no empty space to send frequency hopping signals.

(U) In reply to questions, Rinaldo stated that it was hard to set up the SSB circuits,

except in a narrowband mode, where a synchronizing signal was sent to lock the transceivers before they began hopping. This, he admitted, made LPI mode infeasible, at least at the start of the link. He did not know the efficiency of spectral use provided by SS. No interest in SS was shown by the land mobile radio industry. There was some police interest in secret bumper beepers. Asked about covert use, Rinaldo replied that SS was "not unjammable." (This did not deal with the interception problem). He said that the SS systems that he knew about generally do not live up to advertising, being less hearable by the intended users and more interceptable than the makers claim.

(U) On equipment cost. Rinaldo said slow hopping radios could be cheap if made in quantity, but if a hopping rate as high as 500 Hz was wanted, the cost went up considerably, because of the stricter timing requirements.

(U) The Spread Spectrum column by Hal Feinstein in the AMRAD Newsletter for May 1982 made many of the same points about the lack of enthusiasm for this new technology. The problem of policing Amateur SS led to a concept of a receiver that did not need to know the code for a hopping sequence. AMRAD also discovered that "there are numerous codes which are complex yet do not have privacy properties. So, the number of codes that Amateurs could use is larger than originally thought. If a station illegally uses a complex code to hide the meaning, there are some workable concepts which could be used to detect this."

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

Analysis

(U) The original concept that Amateurs would be able to develop cheap SS radios is unfulfilled. Despite the lack of progress, the development of a circuit board to convert CB radios to frequency hopping would bring the threat of uncontrollable SS radios at low cost back in full force. Once such a circuit board is developed, there will be no practical way to control its dissemination.

(U) The issue of criminal or terrorist use of SS radio techniques that the Amateurs develop has been swept under the rug. The FCC seems uninterested, and the Intelligence agencies cannot touch the problem--unless there is proof that foreign terrorists are using the equipment.

(U) AMRAD has found the "near" problem, viz., SS radiations from a nearby transmitter, to be much worse than expected, practically ruling out any urban or close suburban SS stations. This would appear to undermine the original argument that SS was a good way to increase bandwidth usage, for it interferes with other users more than a narrowband radio would.

(C) The expectation that SS stations would be able to call each other in the SS mode, without a preliminary fixed frequency setup, has been contradicted by experience so far.

[Redacted]

The high cost military SS radios that can call up in SS mode rely on expensive clocks to keep the transceivers synchronized when they are off, and Amateurs generally cannot afford an \$8000 clock to drive a \$300 radio. The technical problems of tight synchronization require severe standardization between all users, and compatible equipment, but Amateurs are usually too varied in their equipment and interests to make this a feasible solution. Hence, it appears that only expensive military SS radios can operate without a proforma fixed channel setup and synchronization.

(FOUO) The interest in "complex codes" that do not have "privacy properties" deserves attention. Because AMRAD has international circulation for its newsletter, and may have foreign members, the experimentation with code generators should be kept within the FCC guidance given in Docket 81-414.

(FOUO) The sale of the 2 meter frequency hopping equipment is also a matter of interest. Who bought it? Who, outside of AMRAD, is authorized to operate SS equipment in the U.S.?

(FOUO) AMRAD's application for a new STA should limit them to the provisions of Docket 81-414, without the release from callup and cipher regulations that was given in the first STA.

(C) Summing up, the attempt to introduce SS on Amateur circuits is off to a slow start, but could still develop if cheap workable modifications for 10 meters (based on CB radios) and for 2 meters are developed and disseminated. There is no visible market for SS equipment or services in any areas where they would overlap existing radio circuits. Some of the enthusiasts apparently want the LPI feature, but have not found the technology to accomplish this cheaply. As long as SS radios are expensive, they can probably be controlled, but will become very difficult to regulate of control if they become cheap.

[Redacted]

The experimenters in AMRAD apparently developed their knowledge of SS technology in government related projects, and are transferring their knowhow. There seems to be inadequate control over this kind of transfer.

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



P.L. 86-36

~~CONFIDENTIAL~~

~~SECRET SPOKE~~

GOLDEN

OLDIE

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



REPORTING
MESSAGE

P.L. 86-36

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

by

[Redacted]

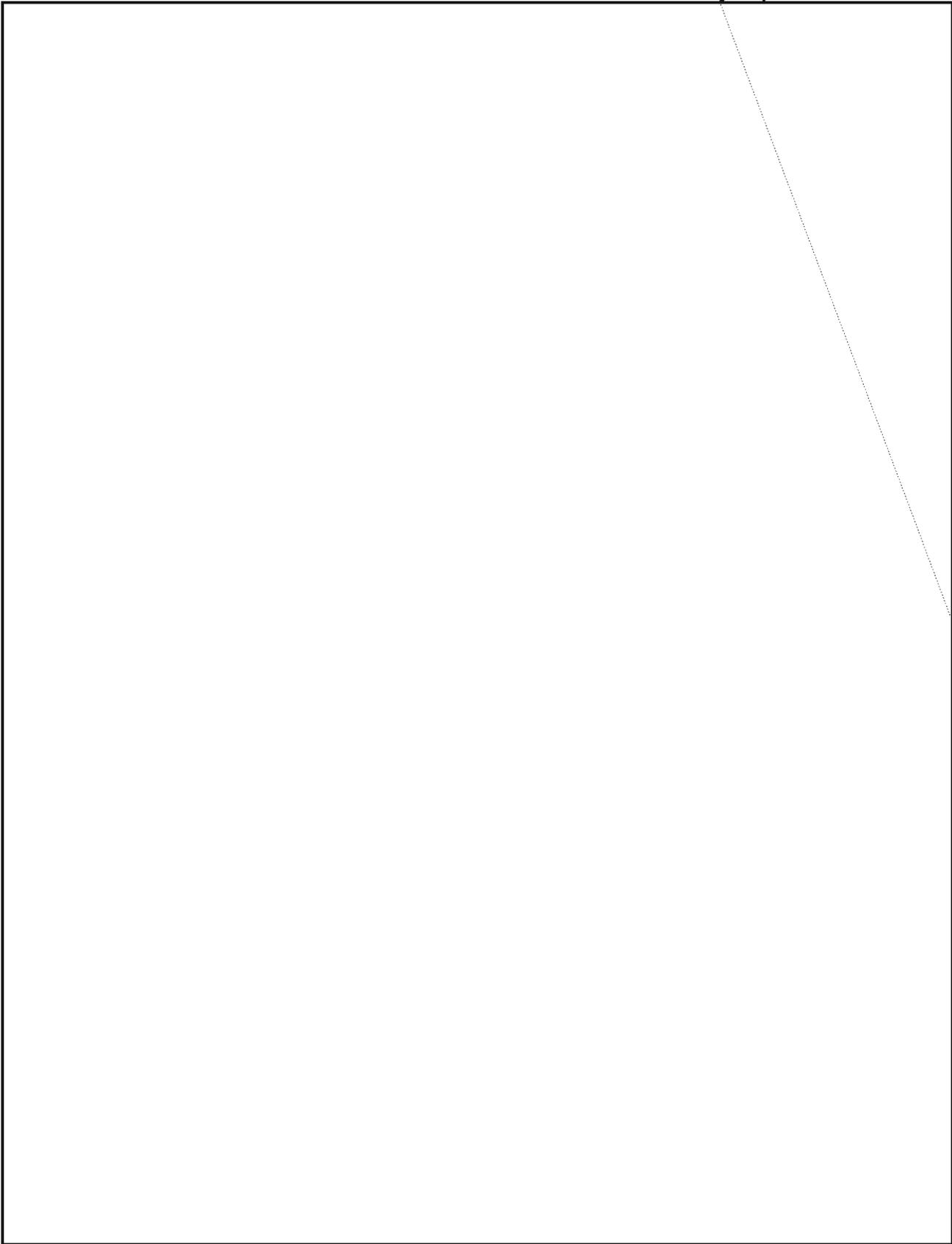
(reprinted from COMMAND, March 1971)

(With grateful acknowledgement to [Redacted])

[Redacted] Donald Oliver, and [Redacted]

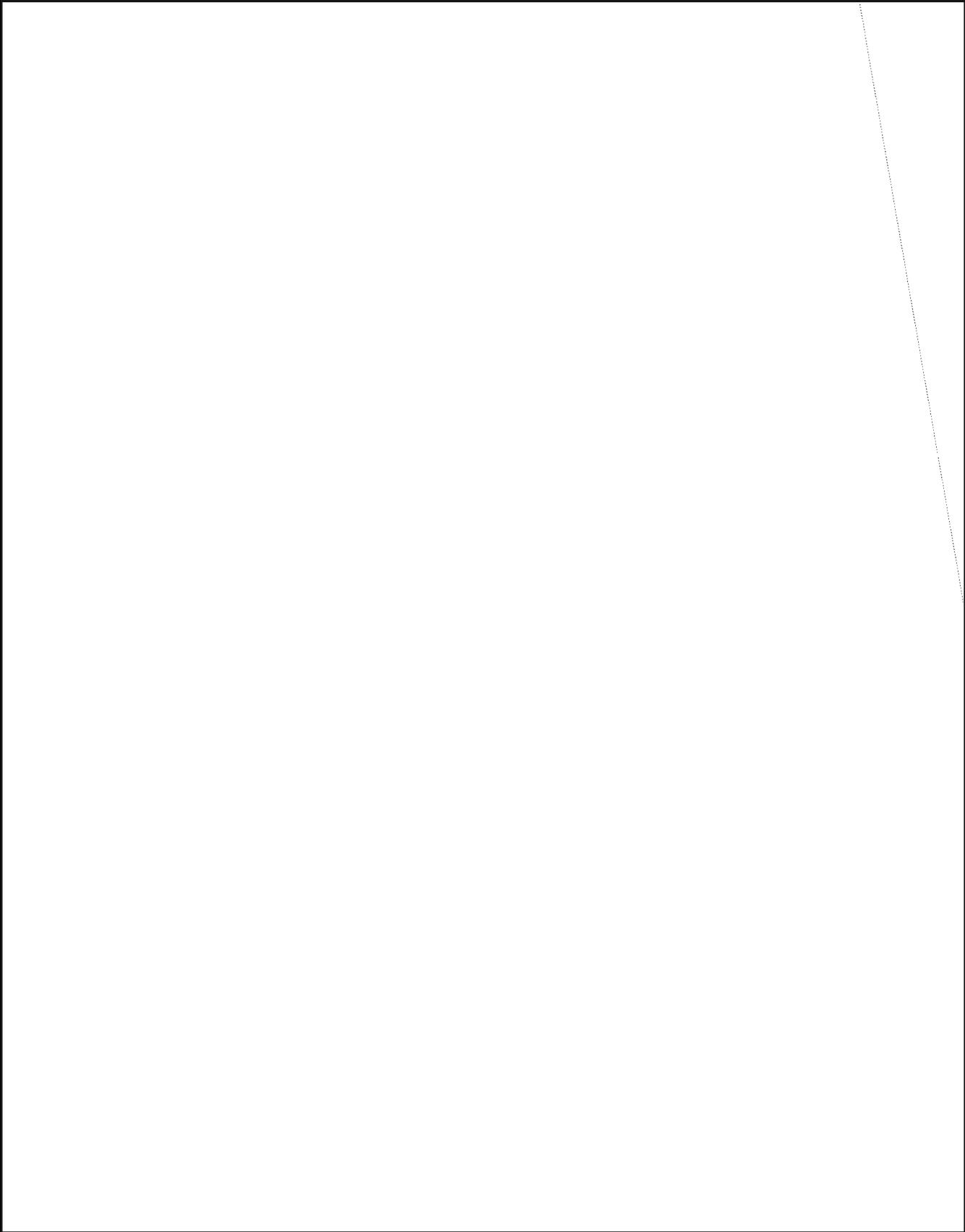
~~SECRET SPOKE~~

~~SECRET SPOKE~~



~~SECRET SPOKE~~

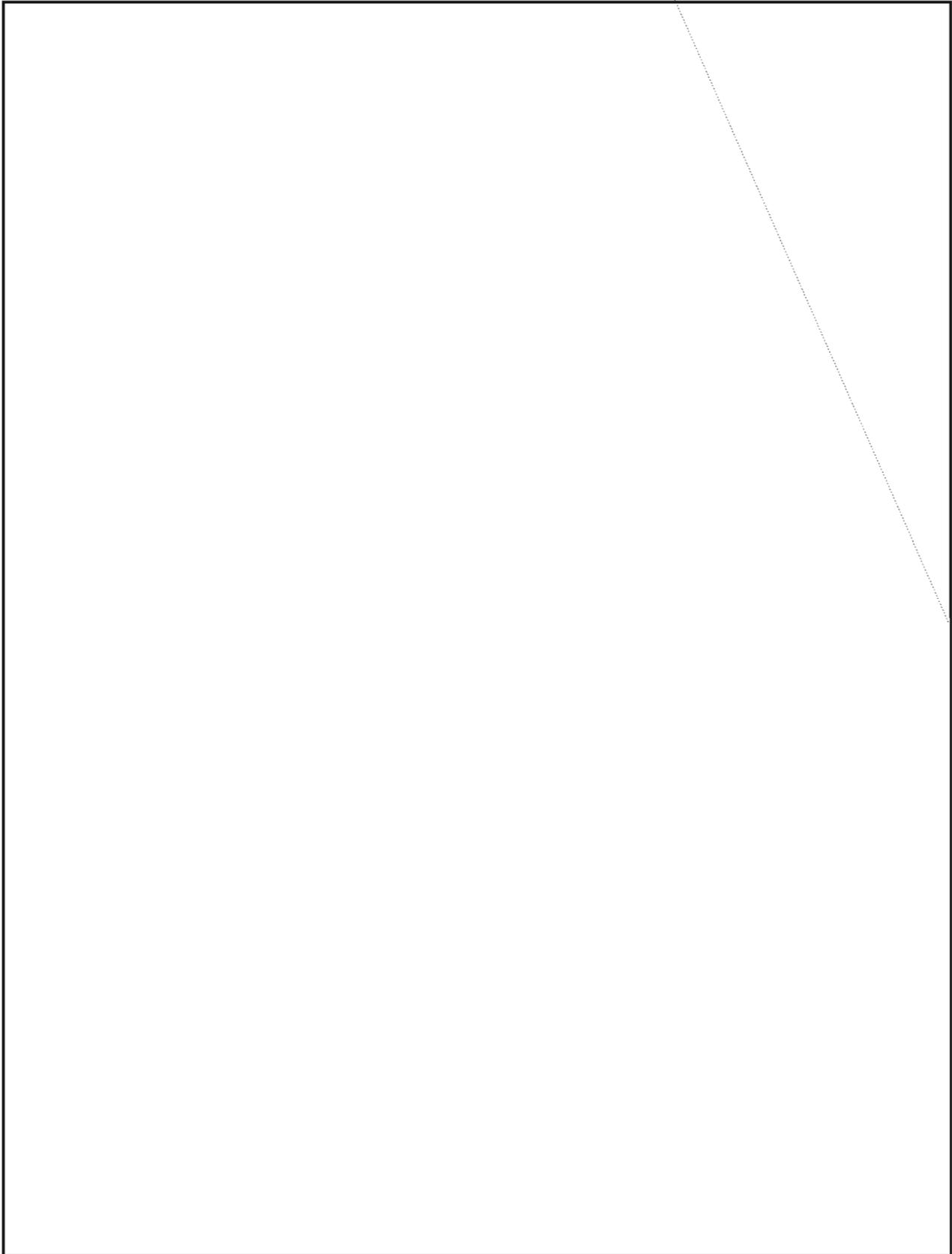
~~SECRET SPOKE~~



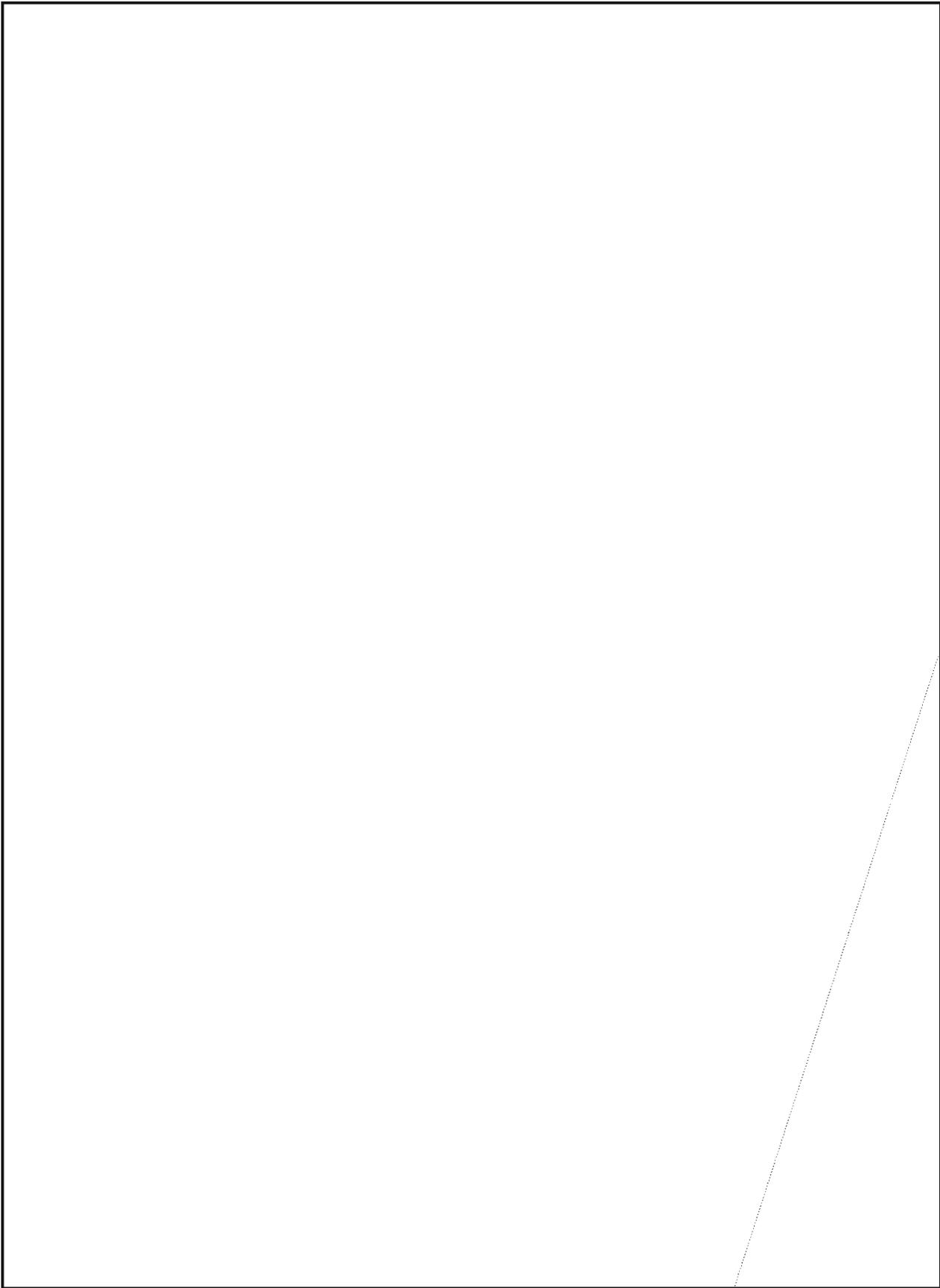
~~SECRET SPOKE~~

~~SECRET SPOKE~~

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

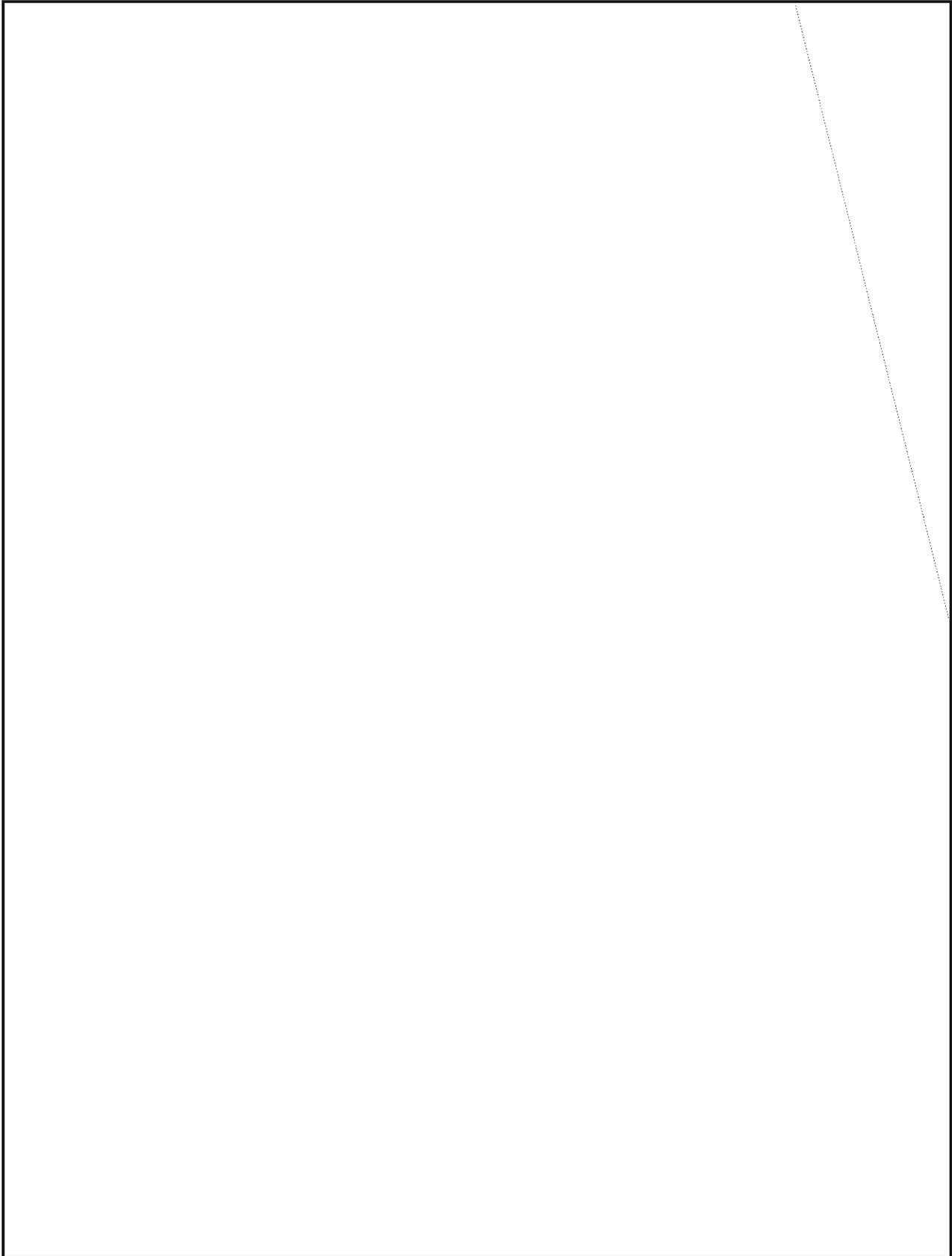


~~SECRET SPOKE~~

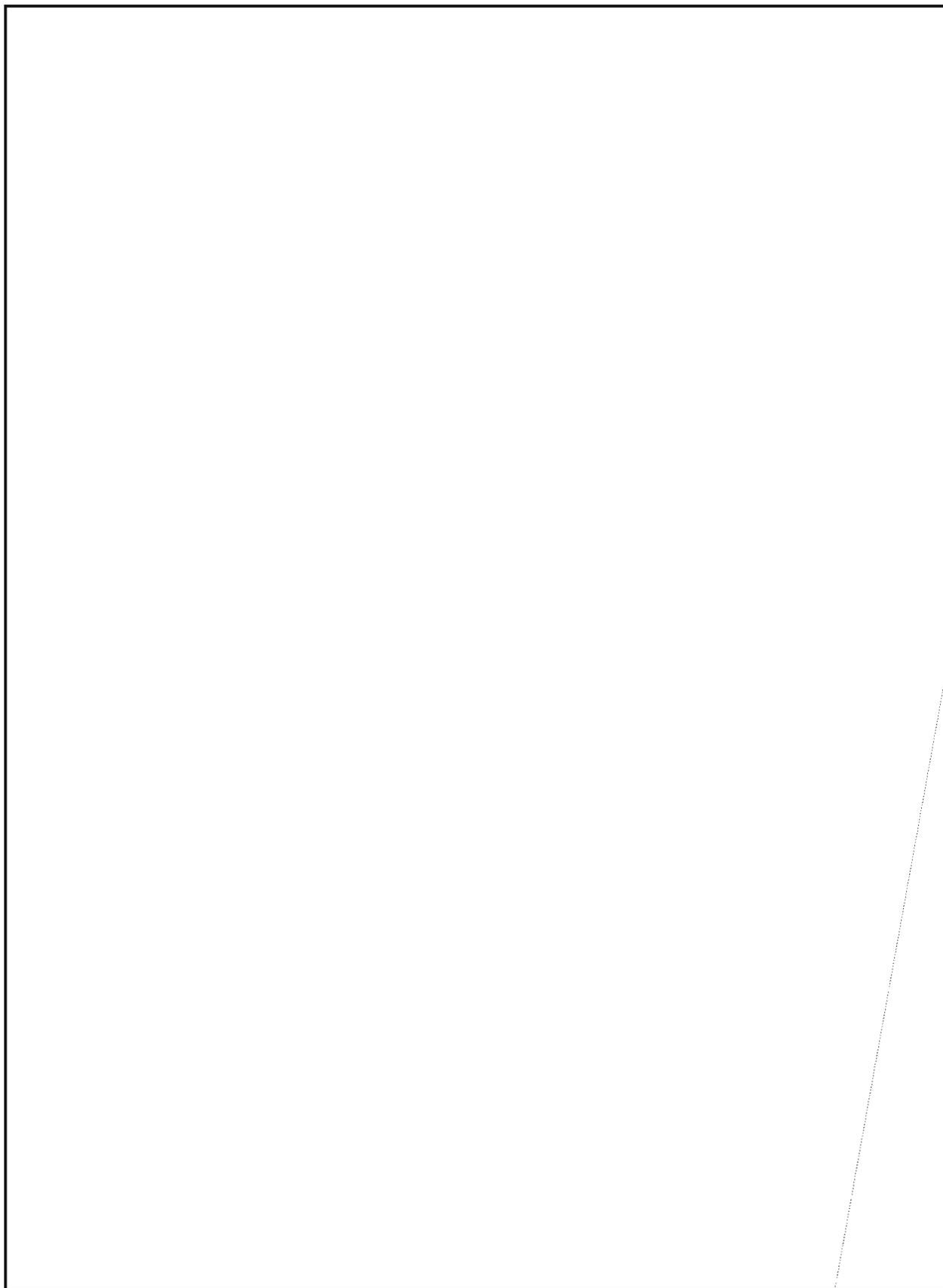


~~SECRET SPOKE~~

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



~~SECRET SPOKE~~



~~SECRET SPOKE~~EO 1.4.(c)
P.L. 86-36

A PERSONAL FOOTNOTE

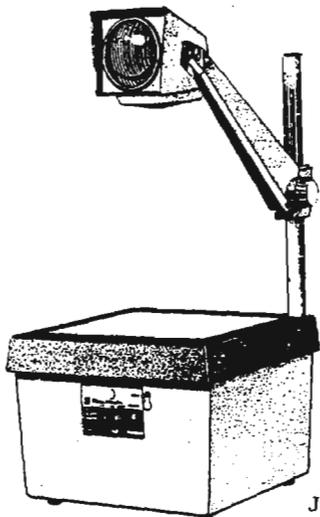
~~(S-660)~~ Early in the war, we were still struggling with how to report in a meaningful way to the customers who wanted daily updates on what we saw in the traffic. The pressure to say something each and every day was overwhelming. One day, a field report came in which argued that troops were coming down through Laos, over the "Ho Chi Minh Trail," and cited increased traffic volumes during certain periods in support of the argument. At the time, there was some collateral information that seemed to support the argument, but as often happens, there was other collateral information that seemed to conflict. The response from the Washington level consumers was strong and immediate: did we agree with the field report?

~~(S-660)~~ The key SIGINT facts in the field report were the message volume numbers, so we began to count. Almost at the outset, problems of method began to surface. We had a large amount of unidentified traffic. Some of the traffic which had been marked as "unidentified" in the field had since been identified. Exactly what traffic did the field analysts count? In the midst of this, we were notified the the Secretary of Defense wanted a personal briefing on the question.

~~(S-660)~~ Communications with the field were not yet as good as they would later become, and there was no easy "opscomm" channel to the people in the field, so that we could talk it over with them. The appointed time for the briefing was only hours away, when, to our dismay, we discovered that different people, counting the same pile of traffic, will usually give different answers, if the pile is large enough. Cut-ins, partial messages, duplicates, circulars to more than one station--all these provide different answers when filtered through the perceptions of different people.

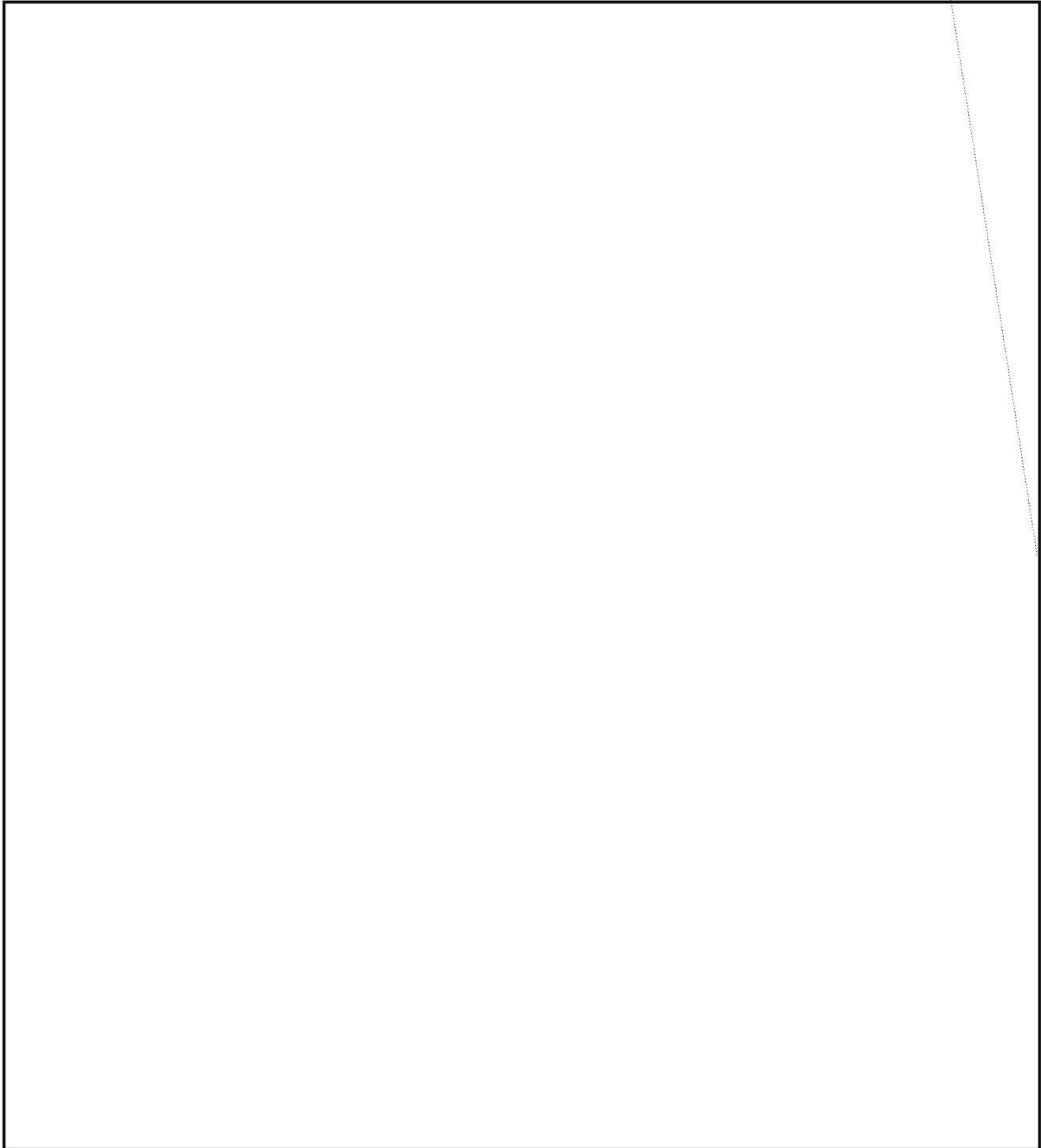
~~(S-660)~~ "Do the best you can." That was the order of the day, and numbers were "developed" for the time period covered by the field report. Then came the briefing of the Secretary of Defense. At the conclusion of the briefing, he said, "Let me have that Vuegraph slide with the numbers on it." And the slide containing those numbers went into his desk drawer. He was, after all, a man to whom numbers were quite meaningful (and he later went on to become a banker). So, we became counters of messages.

W.E.S.

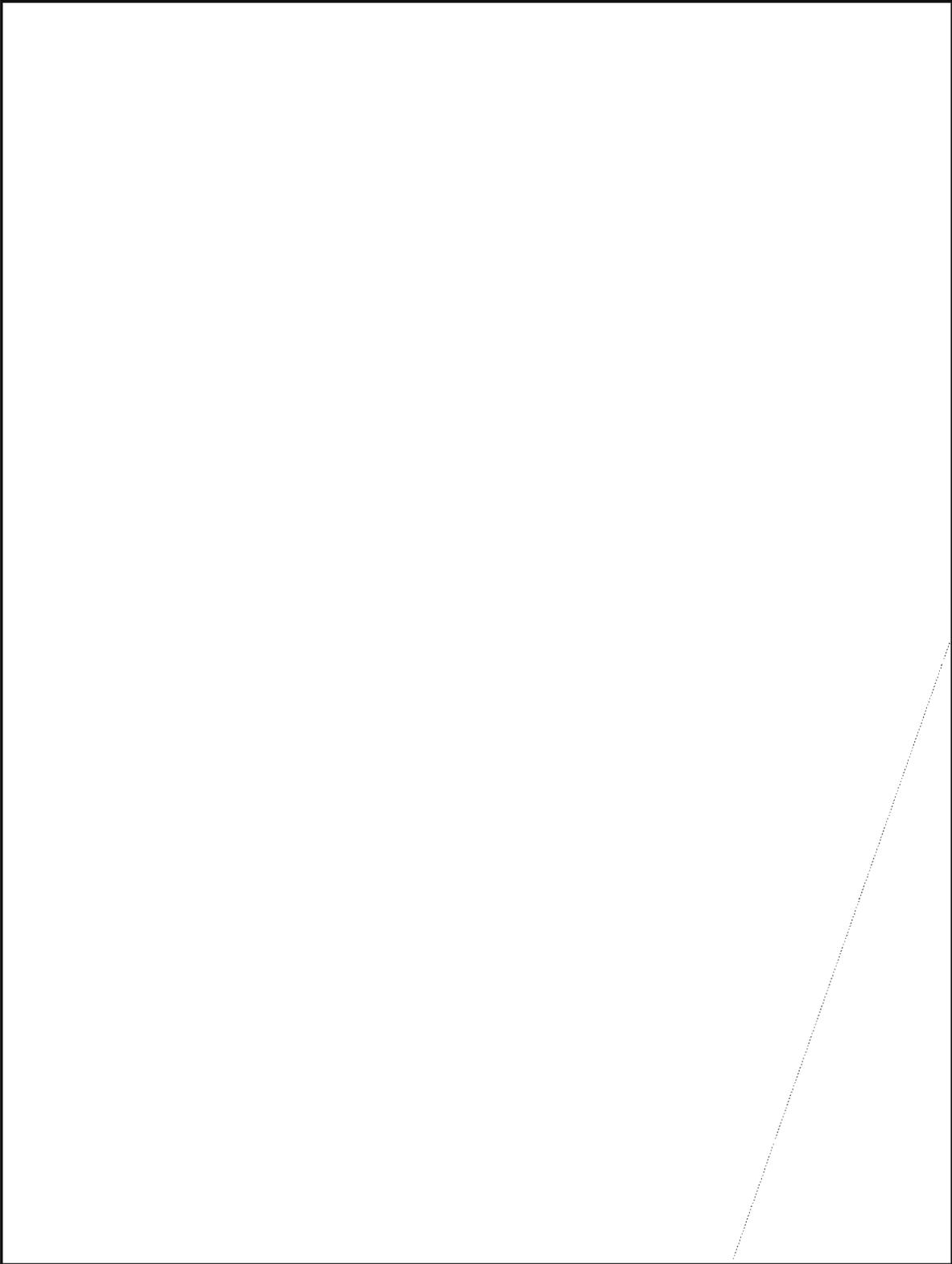
~~SECRET SPOKE~~

NSA-Croctic No.41

THE WORLD'S
GREATEST LIES



UNCLASSIFIED



UNCLASSIFIED

HUMAN FACTORS

Responsible Documentation^(u)



by



P13

P.L. 86-36

REVIEW: "Responsible Documentation", by Neal Margolis, COMPUTERWORLD, 25 January 1982, pp. 7-16

(I wish to thank [redacted] for calling my attention to this excellent article in the "In Depth" feature of COMPUTERWORLD for 25 January.)

natural effect of technological evolution". Cheaper, more widely available hardware is reaching an ever-widening circle of purchasers; increasingly sophisticated and powerful products are reaching more and more unsophisticated users. At today's lower purchase prices, manufacturers are less likely than ever to provide the expensive customer service facilities necessary to reach and support this vast heterogeneous user population. The answer is, (or should be) clear, usable, readable documentation.

■ The customer services staff at a manufacturer of electronic equipment is desperately overloaded with service calls for a new line of equipment--calls that concern minor adjustments thoroughly covered in the manuals.

■ The initially happy purchaser of a new hobby computer gives up in disgust and returns it when he can't get it to perform as advertised, using the elaborate manuals that come with the equipment.

■ A top-level DP consultant contentedly finds himself assured of a long-term job supporting the installation of new software for a large restaurant chain, since he is the only one who can cope with the twelve manuals that make up the primary documentation for the system.

These three apparently different cases have two crucial things in common: they are counterproductive and wasteful for the firms involved and for the users of the products, and they all arise from documentation that fails to carry out its responsibility of communicating to the user. Margolis suggests that "irresponsible documentation is an almost

DOCUMENTATION HAS A JOB TO DO

Margolis makes an excellent point about documentation, in hard-hitting words that make a direct appeal to the manager and the practical businessman: "documentation has a job to do," and it produces a vital output. "Documentation output is in the form of user performance, and by engineering documentation, we can engineer performance." Documentation includes any presentation of information that is intended to improve interaction between a user and a product. It may take the form of manuals, instruction sheets, imprints on hardware that tell how to use it or make it work, or CRT displays that guide a user through a task. Responsible documentation emphasizes what users should do, respects user abilities and limitations, and minimizes "overhead" demands on users (searching, sorting, translating, copying). In contrast, irresponsible documentation focuses on what users have to know, ignores user abilities and limitations, and burdens users needlessly with "overhead" tasks. Spelling out these concepts in more detail, Margolis offers four principles of good documentation design.

MAKE IT ACTION-ORIENTED

Focus on what the user should do, not what he should know. Documentation should approach the user with the assumption that he has specific goals, which were his reasons for buying the product. He doesn't need to read a treatise describing the product or the theory of how it works in some arbitrary text-book sequence. Start with the results or outcomes the user needs, and tell him what he must do to get these outcomes from the product.

"If you want to...., do the following....",
rather than

"The Franistan is connected to the Freeble joint with a red toggle."

Remember, too, that the user's working memory must not be overburdened. He isn't sitting back reading a text book; he is trying to do a task while he follows your instructions, step by step. He needs to see just the statements that apply to the step he is doing, and that answer his questions about that step. Keep the instructions tied to a relevant action the user is to perform, and a small set of concrete events he can see, touch and hear. Margolis adds this warning: don't leave out any user actions or clues because they seem to you (the programmer or engineer) to be "trivial" or "obvious".

"If you don't tell a user to do something, it probably won't get done."

He recommends the use of a systematic method of identifying all the critical cues and actions that will arise for the user. And, last but not least, don't forget that things can go wrong! The user needs to know what can go wrong at each step, and what to do about it.

"Task Analysis" is a systematic procedure for analyzing a user's interaction with a product. Margolis provides an excellent discussion of this procedure, which I recommend strongly to all readers of this review. He describes it as "a procedure that makes explicit each and every action a user must perform to make a product work." The analyst breaks down an overall task into its component steps to produce a list called a task specification. It is spelled out in terms of specific

◆ GOALS (what the user is trying to achieve),

◆ CONDIIONS (events he perceives as cues to trigger an action),

◆ ACTIONS he performs, and

◆ RESULTS (new events he perceives as a consequence of his action).

For example, "When the READY light comes on (CONDITION), push the START button (ACTION) and you will see the message "SYSTEM READY" in the upper left corner of the screen (RESULT)." At this point, a good manual or tutorial should also deal with the possibility that the expected result didn't appear: "If you don't get this message within a few seconds,.....etc."

RESPECT USER CAPABILITIES AND LIMITATIONS

Documentation must take the user's strengths and weaknesses into account.

"Documentation is usually heavily influenced by product experts rather than user experts. Therefore, the common tendency is to assume that the user knows a lot more than he really does."

Too often, documentation reads like an internal technical specification; technical specs are fine in their place, but their place is not in telling a user what to do to get what he wants from a product. A common error is in assuming that "everybody knows" something that, in fact, only technical experts know.

"If you tell a user to do something he does not know how to do, he will probably do it wrong, or he will not do it at all, or he will ask a colleague and the colleague will do it wrong. In any case, either by phone, or in the repair shop, you will have to deal with the problem."

To make documentation fit the user's capabilities, Margolis urges the designer to go back to the Task Analysis. Consider each step, and ask yourself, "Is the user able to understand the purpose of the actions he must perform? How can I make it clearer for him? Will he be able to recognize the conditions that trigger the actions he should take? How can I describe them unambiguously? Will he be able to tell when he has done the action right? Can he recognize the desired result? What if something goes wrong? How can I tell the user

what to look for, so that he knows right away that the action has succeeded, or that it has failed in any of the possible ways it might fail? Finally, can the user do all the actions with the knowledge he has, and if not, what more do I need to tell him?"

Margolis recommends that all design questions be asked with reference to a complete task analysis. This will ensure that all documentation content (pictures, instructions, examples, etc.) is aimed at getting the user to do something rather than just giving him information for its own sake. Secondly, all design questions should be resolved in the context of explicit, detailed knowledge about the user population. He recommends working with a written description of the user, like a set of operating characteristics or specs. This should include the user's education level, professional background, and what he wants from the product. If you anticipate a range of user levels and goals, focus on the least competent user.

MINIMIZE 'OVERHEAD'

Some of the things we ask of the user in documentation relate directly to his interaction with the product, while others relate to his interaction with the documentation itself. The first are vital, while the second are "overhead". These "overhead" tasks may include such things as searching for the meaning of words, sorting task steps that are out of sequence, finding illustrations that are separated from the relevant text, and puzzling over wordy or unclear sentences. The less "overhead" there is in the documentation, the more efficient the user's performance will be. All the principles of clear, readable writing, well covered in many readily-available sources, apply to documentation with even more force than in other contexts. Margolis highlights certain techniques for clear writing as particularly relevant to documentation.

a) Be consistent in using one name for each thing, and make sure that every name or label has a clear reference. Use illustrations generously to make descriptions and labels clear. The article lists a number of common errors to avoid in connection with illustrations, too lengthy to discuss here.

b) Minimize references to information elsewhere (tables and charts, other Chapters or Sections, etc.), especially if the referenced data is something the user has to have to complete a task. Put as much as possible "in

line", at the place where the user needs it. Avoid at all costs using any "implied reference"--a term, concept, or bit of data that the user needs, but that you have forgotten to include, or that you assumed "everybody knows"! A motivated user will search diligently, paging through your documentation as he tries to find the missing data; his task and his flow of thought are both disastrously interrupted for long periods of time. He will rapidly lose respect for the documentation, and his distrust will extend to the product as well. A non-motivated user (or one who has been "burned" once too often already by your documentation) will give up and gripe.

TEST DRAFT DOCUMENTATION IN ADVANCE

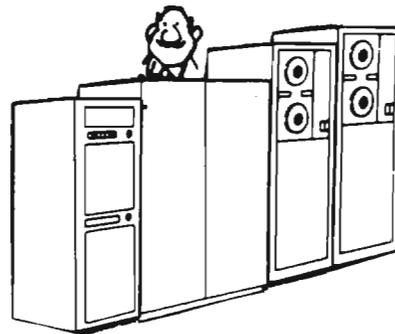
Test the documentation carefully before you deliver it or the product. "Get some people who represent your user population; users. Have them work through several sample problems, and watch every step they make. When they stumble, ask them why. Take lots of notes. When you discover big problems with the product (not just the documentation!), either correct them or let the user know what he has to do to avoid them."

DON'T TRY TO 'ECONOMIZE' ON DOCUMENTATION

Margolis emphasizes the fact that documentation produces a measurable, accountable output. Before a final commitment is made on documentation content, format, and organization, it must be tested, and its output measured. If it isn't performing well in improving the relationship between user and product, it must be revised.

"Too often, 'validation' means a technical review by engineering personnel in order to verify the accuracy of the material."

You should make an explicit commitment to test the documentation, with real users in real situations. Go back to the all-important task specifications that should have formed a basis for the documentation. Measure user performance in the test against the performance standards spelled out in the goals, conditions, actions, and results of the task analysis. Use draft versions of the documentation, with full expectation of having to change things. Watch the users during the test, and talk things over with them. "Saving" time, effort, and money by skimping on documentation is the reverse of economy from any but the most short-sighted point of view.

~~CONFIDENTIAL~~

Some Reflections on the Reality of Computer Security (U)

by Robert J. Hanyok, H215



Along with the tremendous growth of our computer usage in recent years, we have become aware that we need security measures that will protect the computer, databases, and associated programming. We have developed a host of techniques and plans in response to this need, including access restrictions, passwords, audit trails, encryption, etc. Security officers have been generally enthusiastic in carrying out these measures. As a result, the users have insisted that the resulting security of their systems is ironclad and invulnerable. On paper their claims seem valid, but beneath those claims is a reality that belies this so-called "security."

(U) Here I should establish two points. First, this paper is a personal impression of computer security practices. It is not an analysis of particular security modules, equipments, or kernels; nor is it intended to be exhaustive in scope. The aim is to illustrate the so-called human factor shortcomings I have encountered, examples of which all occurred on computer systems having one or more security measures.

~~(C)~~ Second, my observations are based on more than two years' work in the S organization, where I was involved in evaluating the security frameworks of various computer systems used by NSA, DoD, other federal agencies, and by contractors. I helped develop the Computer Security Survey System (CS²) which became a major tool in analyzing the security elements of these systems. CS² provided a prioritized, coherent, and quantitative method of evaluating computer system security. The use of CS² provided, for me, the first inklings of the reality of computer security practices.

(U) Just what is the reality of computer security? The reality is that computer security measures are often undercut by user practices and less-than-adequate implementation. There are three elements to this reality that I have observed. To a degree they are interactive. They all have one trait in common: they are not obvious in a system level review.

~~(C)~~ User level security practices vs. system level security measures.

The user does not fully use the security measures that are available on the computer system. Some techniques, like audit trails, are now controlled by the system and operated with the user ordinarily unable to intervene, alter, or negate them. But some measures, by their nature, allow the user much latitude. The most common case I encountered was with passwords. Some systems levied length requirements for passwords; some did not. Source and randomness of passwords were ill-defined. The result, of course, was that while everyone had passwords, they could be too few characters, predictable, and often kept in accessible places. In one office we visited, the operators had taped their passwords to the terminals. In another system, unauthorized persons were given passwords for "special projects." At best, such practices can be labelled sloppy; at worst, they are an outright invitation to compromise.

~~(C)~~ User security practices are dictated, not by the classification level of the data, but by the perception of the threat.

This was probably the most unexpected phenomenon I encountered--almost a reversal of conventional security imperatives. While some users who handled sensitive data in their

~~CONFIDENTIAL~~

computers seemed to give it proper protection, the rest (i.e., the vast majority) did not. Instead, they protected their data, including caveat, codeword, and compartmented material, only to the degree needed to defeat what they perceived as the threat. This practice would not be a problem if the users were conscious of the constant real threat to their material. However, the normal attitude encountered during CS evaluations was that

"Our computers operate in a benign environment. Why do we need these protective features?"

A so-called "benign environment," is one like the physical environment of NSA with its wire fence, guards, badges, etc. But it is only an illusion of security, because we know that "cleared" personnel continue to be targets of recruiting by hostile foreign intelligence. Because of this Pollyanna attitude, sensitive material is placed in computer systems whose protective features are either less than adequate or nonexistent. The data on a system is available to anyone who can access that system.

(C) Both partially secure or unsecure computer systems allow conventional security safeguards to be circumvented.

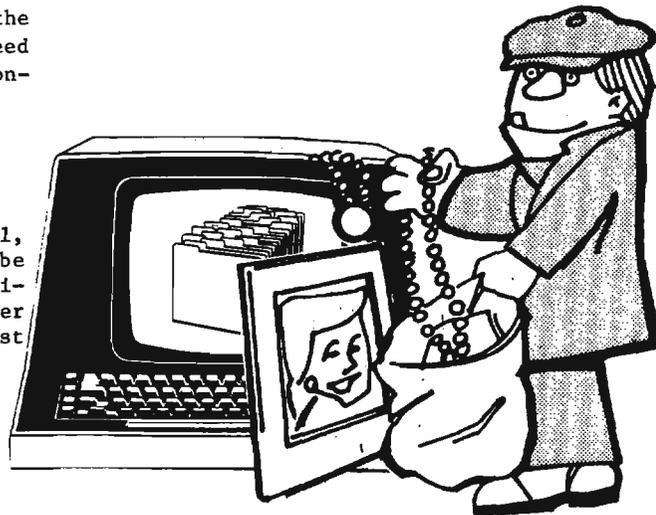
Remember the offices handling sensitive data? They had the full panoply of special security: locked doors, sign-in lists, escort requirements, and special clearances. Yet these same offices would place the same sensitive data in an unprotected computer file space that was accessible by anyone on the same system. Deterred by physical controls, an individual could still retrieve the data through the computer. The special feature of this element is remoteness. The distance involved between the data and the person getting access to it need be no closer than the furthest terminal connected to the computer holding the data.

(U) If the problem is at the user level, does it then follow that the solution may be there as well? In a word, yes. It is critical that the effort directed towards computer security reach the user. Solutions must include him.

(U) First, programs should be set up that will make the user aware of the real threat to his system. A basic course on computer security, or a computer security portion of Agency on-board briefings would be helpful, but this would take time to carry out. As an interim solution, computer system security officers could draw up security/threat briefings which would be mandatory for all users of their system. All new users should be given a brief of this sort as a prerequisite to operation.

(U) As a second solution, those individuals who manage resources at the user level (i.e., branch, work center, team) could be given computer security responsibilities. This should not dilute the system security officer's job in any way. If anything, this could extend his effectiveness to the local level where it can do the most good. In this proposal, the local resource manager, acting for the security officer, would be responsible for assuring that security measures are carried out at his level. His proximity to the user can help to eliminate the problems cited earlier. This security task is hardly onerous--after all, he is assuring that already issued security requirements are being met. He represents a form of insurance that we need for computers.

(U) No computer system is absolutely impervious to attack. But it is also true that failure to assure even basic security can circumvent the best computer security measures, through a lack of awareness or responsibility. The commercial computer world is replete with incidents of embezzlement, intrusion, deception, thievery, and sabotage. Can we honestly expect less of a threat to our computers?





means that our deadline for material is roughly the 10th of the month, give or take a day for intervening weekends. If you want to get something into a specific issue, give us a call and let us know how much space to hold for you.

~~(FOUO)~~ This is the time of the year for coming and going, so a word about the distribution of CRYPTOLOG might be useful.

~~(FOUO)~~ Our distribution is to organization and to individuals within the NSA headquarters, and to organization only outside the immediate area of the headquarters. Because of the technical nature of the various articles and items in CRYPTOLOG, it should not go outside the technical community. Even articles that are marked as UNCLASSIFIED should not be taken outside the work area, unless cleared by [redacted] Q44, x3085s or 688-6524 (see CRYPTOLOG, May 1982, page 4, fourth paragraph).

~~(FOUO)~~ When subscribers move to a job outside the headquarters area, we can send the magazine to the organization, but not to the individual. When you return, a phone call or note to [redacted] P14, Room 8A177, x3369s, will get you back on the distribution list by name.

(U) Until now, the month that each CRYPTOLOG issue carries on the cover has been the month we go to press, but this has been confusing to some, because the readers didn't see the issue until the following month. Thus, the April issue didn't appear on your desk (or wherever you get your mail) until May. So, this issue becomes the June-July issue, and future issues will carry the name of the month in which (we hope) they appear.

(U) We have been sending each issue to the printer somewhere around the middle of the month, and the process of printing and distributing has been taking about a month. This

Solution to NSA-Croctic No. 40

"Rules for the Camel Corps,"
[redacted] CRYPTOLOG,
March 1982

"It is frightening to contemplate the amount of time [we] NSA employees spend in meetings. There are staff meetings at all [echelons], meetings to solve a particular problem, club meetings, and even meetings to find reasons for more meetings. 'He's at a meeting' is all too frequently heard on the other end of a phone call."

P.L. 86-36

From: phr at CARONA
Subject: Editorial comment
To: cryptolg at barlc05
cc: phr

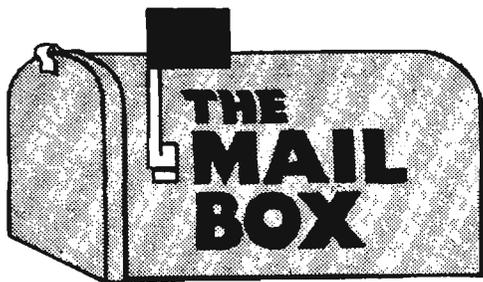
Hi,

(U) Just received my May 1982 issue of Cryptolog and read with suprise the editorial on moving. I would like to share with you my theory on the need to keep moving within the Agency. Clearly, there is at least one too many organizations in the Agency. Therefore, it is imperative to keep one organization in a moving van or stacked in the halls at all times. I am astonished that in all your years at NSA, you have not reached this same logical explanation. NSA is a giant version of one of those puzzles that have 35 numbered sliding pieces with one blank hole. SOMEONE is trying to get all the offices into numeric order but the speed with which we reorganize around here constantly frustrates THEIR efforts and causes the constant moving we MUST ENDURE.

Thank you,

[redacted]
T441, 1181s
phr@carona

P.L. 86-36



From: phr at CARONA
To: cryptolg at barlc05
cc: phr

(U) Read with interest your article on Shell-Game in the latest issue.... I think the response you get to this feature will overwhelm you!!!

Sincerely yours,

[Redacted]
T441 1181s

EO 1.4.(c)

Dear Editor,

~~(C)~~ I read in the April 1982 issue of CRYPTOLOG in the article on "PERSONAL COMPUTER APPLICATION" by Richard J. Fitzpatrick, P13, about a problem in converting Universal Transverse Mercator (UTM) grid coordinates to latitude and longitude in Geographic grid coordinates. This problem had been solved in June 1970, and three hard copy working aids (WA) were prepared showing machine generated UTM to Geographic coordinate conversions for South Vietnam (B63 WA #22-70, dated 17 July 1970), Cambodia (B63 WA #23-70, dated 17 July 1970), [Redacted]

[Redacted] These were very popular documents and the working aid for South Vietnam became a "best seller." It was originally published in 290 copies and was provided to traffic analysts and special research analysts at NSA and field stations. As soon as it became available, the response was overwhelmingly favorable and many requests for additional copies came from field stations and NSA elements. It was used daily and, being made of paper, it wore out and needed replacement. By the time I left B63 in March 1972, we had provided approximately 1000 copies of this working aid.

~~(FOUO)~~ This program which converts UTM coordinates to latitude and longitude on a personal computer will be of immense value to all target areas.

[Redacted]
B32 5189s

From: jwh at CARONA
Subject: Games with Shell
To: cryptolg at barlc05

P.L. 86-36

(U) I enjoyed your article on using shells in the recent CRYPTOLOG. I understand [Redacted] did as well since he sent you his "who" shell (I have a better one yet). I thought you might be interested in the following loooong shell. [Redacted] asked me to produce a program that a user could run against his/her own account to show what files (if any) were open to other users on the system. I decided to do it all in shell in case other users wanted to modify it. Granted it takes some time to run, but it works. There may be some who would want it to do more, however I think it proves that almost anything can be done with shell.

[Redacted] T442/x5553s

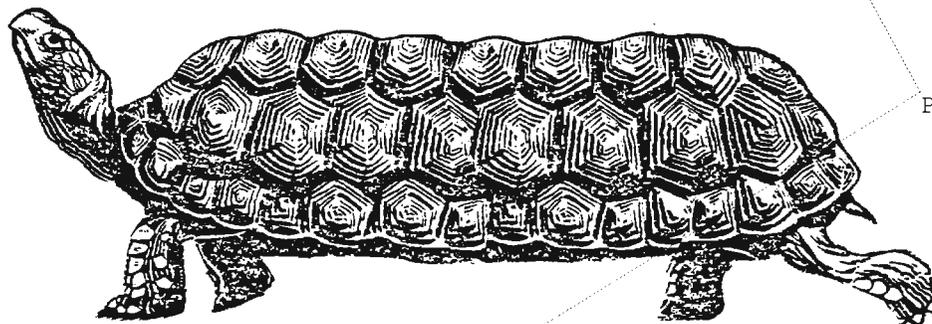
(Ed note:
See the shell expose beginning on page 27.)

A LOONG SHELL (U)

by



T4



P.L. 86-36

```

echo Expose: vl.3 Tue Sep 8 15:34:24 EDT 1981
: comment - This program was authored by [redacted] at the request of
: comment - Bernard Peters the SENIOR COMPUTER SECURITY COORDINATOR.
: comment - The purpose of the program is to search through a users
: comment - directories and report to the user those files that are
: comment - open for read/write by anyone on the system and other members
: comment - of the users group the program will also inform the user
: comment - who the members of his group are because most dont know.
: comment - This routine tells the user what the program will do.

echo This program will examine your Directory and File systems to identify
echo "      Files which can be READ or WRITTEN by others:"
echo " "

: comment - Check to see if the user wants the file exposed.files removed
: comment - if it already exists. If not and exposed.files exists the
: comment - program will exit and notify the user.

if $1: = -: goto killfile
if -r exposed.files goto anyout

: comment - Routine to get the users current program work directory name
: comment - and search the users files and directories from the login
: comment - directory of the user.

: killfile
echo Getting your directory information:! >exposef$$5
tr "!" "203" <exposef$$5>exposef$$6
cat exposef$$6;rm exposef$$5 exposef$$6
pwd >exposef$$8
cat exposef$$8 | reform +t8 | rpl "^" "lz -lxp " > exposef$$1
sh exposef$$1 | sort +.41 > exposef$$2
echo "      "

: comment - The users files and directory name are now placed into the
: comment - line editor where those files in question are extracted
: comment - and placed in an output file called exposed.files.

ned - exposef$$2
l,$s/ .*://g
l,$s/total.*//g
w exposef$$2

```

```

1,$g/exposef/d
$+la
Files readable by anyone:
.
$1
$d
1,$g/^.....-/d
1,$g/^.....r/1
1i

```

For those who don't like to type,
this shell can be found on CARONA as
/u3/jwh/misc/expose

Files readable by anyone:

```

-----
.
1i
$kg
'gr exposef$$2
$+la
Files writeable by anyone:
.
$1
$d
'g,$g/^.....-/d
'g,$g/^.....w/1
'g+1i

```



Files writeable by anyone:

```

-----
.
1i
$kg
'gr exposef$$2
'g,$g/exposef/d
$+la
Files readable by anyone in your group:
.
$1
$d
'g,$g/^....-/d
'g,$g/^....r/1
'g+1i

```

Files readable by anyone in your group:

```

-----
.
1i
$kg
'gr exposef$$2
'g,$g/exposef/d
$+la
Files writeable by anyone in your group:
.
$1
$d
'g,$g/^.....-/d
'g,$g/^.....w/1
'g+1i

```

Files writeable by anyone in your group:

```

-----
.
w exposed.files
q
echo " "
echo " Change unsatisfactory access codes, use CHMOD "
echo " " >> exposed.files

```

```

echo " Change unsatisfactory access codes, use CHMOD          " >> exposed.files

: comment - This sub routine searches the files etc group to find out
: comment - the login names of the other members of the users group
: comment - and then does a wru against the login to show the user
: comment - the full name of the other members of the users group

echo Determining who your group members are                    ! >exposef$$5
tr "!" "203" <exposef$$5>exposef$$6
cat exposef$$6;rm exposef$$5 exposef$$6
cat exposef$$1 | reform +m12 | rpl "^" "grep " | rpl "/" "" > exposef$$3
ned - exposef$$3
l,lt2
ls/$/,/
2s/$/\
l,2s/$/ /etc/group/g
w
q
sh exposef$$3 > exposef$$4
ned - exposef$$4
$1
T44:,
.
l,$s/.*://g
l,$s/,/ /g
l,$g/^ /d
w
q
cat exposef$$4 | tr " " " 12" > exposef$$10
cat exposef$$10 | rpl "^" "grep " > exposef$$11
ned - exposef$$11
l,$s/$/: /etc/passwd/
w
q
sh exposef$$11 > exposef$$12
ned - exposef$$12
l,$s:/ /g
l,$v/-/d
w
q
cat exposef$$12 | usort > exposef$$5
echo " "
echo " " >> exposed.files
echo " These are the group members who can access your files:"
echo " These are the group members who can access your files:">> exposed.files
echo " "
echo " " >> exposed.files
cat exposef$$5 | tee exposed.files$$
cat exposed.files$$ >> exposed.files ;rm exposed.files$$
echo " ";echo " " >> exposed.files ;echo "This list made " >> exposed.files
date >> exposed.files ;echo " "
echo "The list of files accessible by anyone is now in your file: exposed.files"
chmod 600 exposed.files;rm exposef*
exit

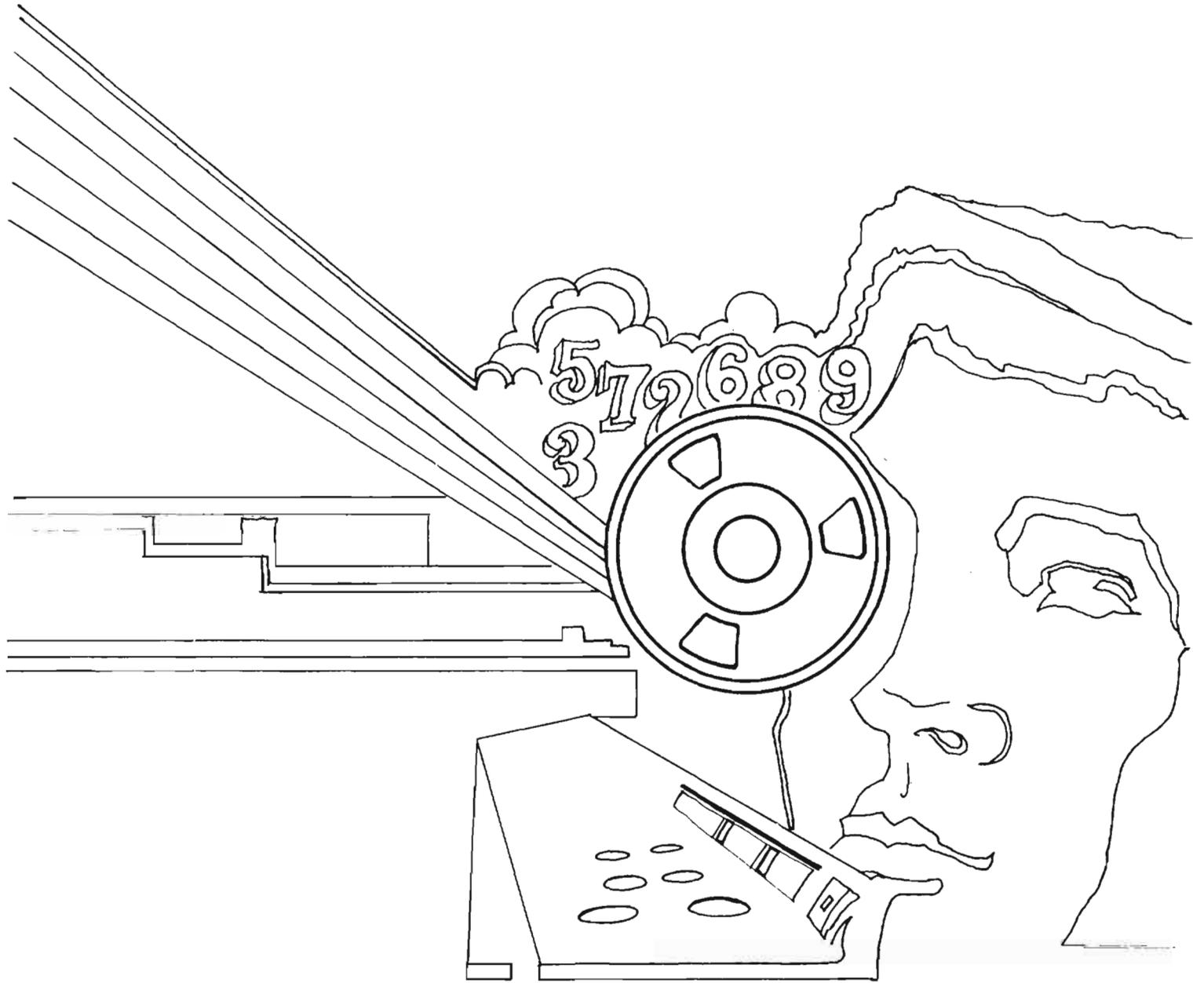
: comment - ERROR sub routine to notify the user that the exposed.files
: comment - already exists.

: anyout
echo "EXPOSE ERROR:";bells 1
echo " The File 'exposed.files' already exists -- this file must be"
echo " re-named or removed before -expose- can run"
echo " or run 'expose -' which ignores the file's existence";bells 1
exit
Tue Sep  8 15:34:24 EDT 1981

```



~~SECRET~~



~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~SECRET~~