TOP SECRET

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

2nd Issue, 1988

P.L. 86-36

THIS DOCUMENT CONTAINS CODEWORD MATERIAL

TOP SECRET

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

NOT RELEASABLE TO CONTRACTORS

DOCID: 4019715

CRYPTOLOG

P.L. 86-36

Published by P1, Techniques and Standards

VOL. XV, No. 2............................ 2nd Issue 1988

PUBLISHER.........................

BOARD OF EDITORS

Editor .... (963-1103)

Collection .... (963-5877)
Computer Systems .... (963-1103)
Cryptanalysis .... (963-5238)
Cryptolinguistics .... (963-4740)
Index .... (859-4351b)
Information Science ...... (963-3456)
Information Security .... George F. Jelen (972-2122)
Intelligence Research ... (963-3845)
Language .... (963-3057)
Mathematics .... (963-5566)
Puzzles...... .... (963-6430)
Science and Technology .. (963-4958)
Special Research .... Vera R. Filby (968-8014)
Traffic Analysis .... Robert J. Hanyok (963-4351)

Illustrators .... (963-3057)
.... (963-4989)
.... (963-3738)

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

If you used a word processor, please include the mag card, floppy or diskette along with your hard copy, with a notation as to what equipment, operating system, and software you used.

via PLATFORM mail, send to:
c r y p t l g @ b a r 1 c 0 5
(bar-one-c-zero-five)
(note: no 'o')

Always include your full name, organization, and secure phone; also building and room numbers.
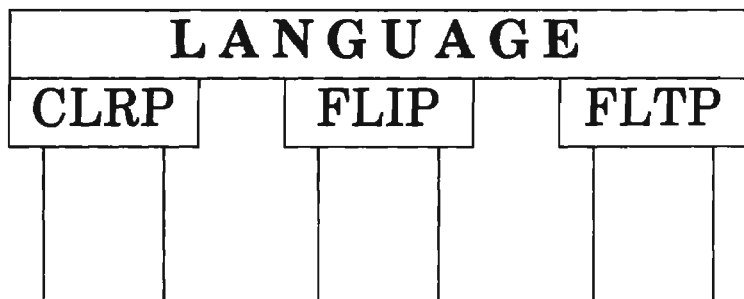
For Change of Address
mail name and old and new organizations to:
Editor, CRYPTOLOG, P1, HQS 8A187
Please do not phone.

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

All opinions expressed in CRYPTOLOG are those of the authors. They do not represent the official views of the National Security Agency/Central Security Service.

THE GENTRIFICATION OF NSA

NSA is growing in leaps and bounds, as you can see from the many trailers to house operational elements that have been springing up like toadstools after a rain. Only temporary quarters, they assure us. But history tells us otherwise. The WW I temporary structure on the Mall known as the Munitions Building housed our predecessor in the early days of WW II and survived for half a century. At Arlington Hall, the temporary buildings of WW II that were NSA's first home will soon have their golden anniversary.

So we may as well recognize that "temporary" buildings associated with us are only relatively so—compared to the pyramids, that is—and incorporate them into the grand design.

The makings of a charming Olde Worlde enclave, a walled city, are already in place. There are rudimentary Grand Plazas at the entrances of Ops 2b and the HQS buildings. There's an attractive (well, mostly so) courtyard between the two new buildings and Ops 1. All that's needed is gentrifying the trailers: a few petunias here, the odd geraniums there, and imaginative paving joining the trailers to the main buildings. Hardest of all is deciding whether the paving should be patterned brick, a design in terrazzo, or even, log slices set in gravel, Japanese style.

FOR OFFICIAL USE ONLY

Three Programs in Support of

G7

LANGUAGE
CLRP   FLIP   FLTP

THIS ARTICLE IS CLASSIFIED ~~CONFIDENTIAL CCO~~ IN ITS ENTIRETY

An ongoing problem at NSA has been staffing language positions and encouraging linguists to remain in the language field once they fill these positions. The Agency has looked at this problem through several studies and has implemented a number of programs in an effort to alleviate the problem.

Historically, at NSA there has been a great imbalance between the workload and the workforce in language.

Despite the expanded needs in language, however, the language workforce has tended to remain relatively static. Until recently, linguists at the grade 12 level were changing to other career fields or going into management positions in order to progress to higher grades, as they felt that there was no potential for advancement in language.

Attrition of linguists has been of great concern, since departing linguists often represent the sole source of a language skill, and are therefore considered irreplaceable.

To solve this problem, Section 10 of the National Security Act of 1959 was amended to grant the Director the authority "to establish and support language and language-related training programs for civilian and military cryptologic personnel, provide special incentives, allowances and benefits to personnel in language and language-related skills, provide language training to families of designated personnel, and establish a Cryptologic Linguistic Reserve Program." The Agency thus hoped to make available sufficient language resources to provide for current as well as anticipated needs.

Several programs have been instituted as a result. Incentives, in the form of specialized training or pay, were established by NSA/CSS Directive No. 40-1, dated 6 May 1982, and include the three programs described in this paper: the Cryptologic Linguist Reserve Program (CLRP), the Foreign Language Incentive Program (FLIP), and the Family Language Training Program (FLTP).

## The Cryptologic Linguist Reserve Program

The CLRP was implemented to provide for a reserve pool of individuals with specific language experience whom the Director can call upon in emergency situations. It responds to the problem of attritting linguists whose departure leaves the Agency with little or no resources in a particular language. This group consists largely of former or retired civilian or military cryptologic personnel from the Agency, but may also consist of other individuals who the Director determines to be qualified. Members of the CLRP "agree in writing to serve for a period of one year, to serve in an active civilian status with the Agency during

EO 1.4.(c)
P.L. 86-36
DOCID: 4019715

periods of emergency, perform such linguistic or linguistic-related duties as the Director may assign, maintain their language skills as required, and accept such training as is required."

The program is limited to persons possessing knowledge of a Class I or Class II foreign language or one required by the Agency for crisis situations.

Prospective members must have worked with the language within the past 18 months or must have passed the appropriate Language Proficiency Test (LPT).
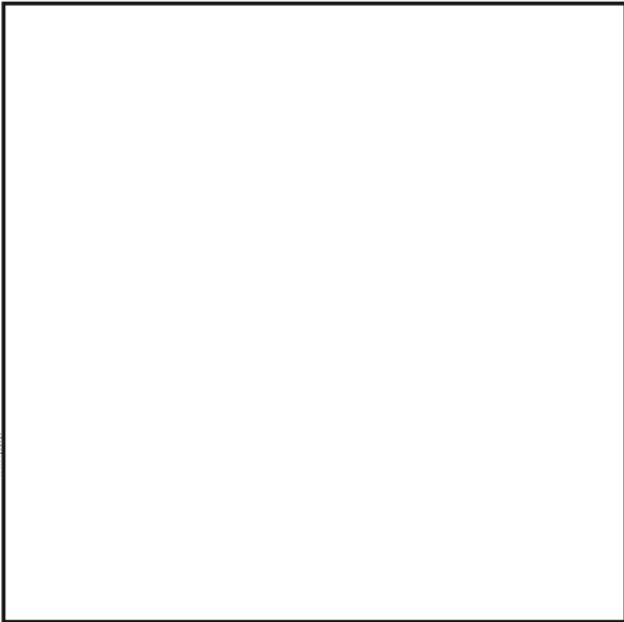
The CLRP is under the management of the Deputy Director for Administration (DDA.) However, it is the Deputy Director for Operations (DDO) who is responsible for informing the Director of an emergency situation that warrants the call to duty of members of the CLRP, as well as for establishing a priority listing of Class I and II languages requiring augmentation in a crisis situation. This listing includes the number of CLRP personnel needed in each language and is to be provided to the DDA and Assistant Director for Training (ADT). The Deputy Director for Programs and Resources is responsible for reviewing the manpower requirements for the CLRP and advising as to the availability of funds for the program.

P.L. 86-36

Previously, individuals to be offered membership in the CLRP were recommended by chiefs of key components to the DDA. To help in the selection process, M3 circulated listings of recently separated employees to offices for their endorsement. In May 1986, however, a change was made from soliciting individual linguists to circulating information about the program to exiting GGD-07 and above personnel. A brochure was designed in late 1985, but as of mid-1987 it has not been published, largely for lack of funding. Nevertheless, in anticipation of the new system, the practice of circulating listings of separated employees to appropriate offices was dropped in July 1985.
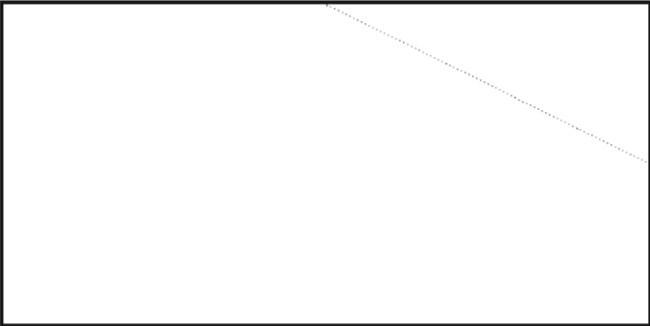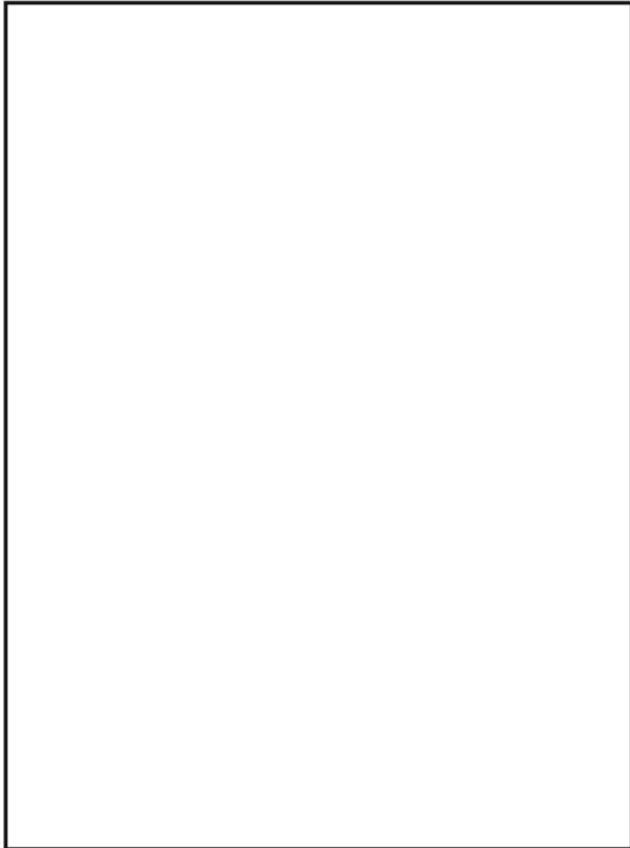
P.L. 86-36
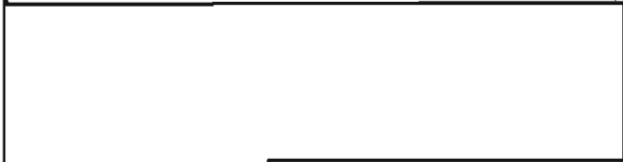
Members of the program are initially tested for proficiency and are to have follow-up testing or training after two years in the program. The program calls for members to be brought back for periodic training or operational assignment.

One of the main problems is that while the statute establishing the program calls for some sort of training after two years, it is not being done: three members have been in it long enough to be receiving this training, yet there is none available. M3J is still waiting for G Group to compile a training package.

The Foreign Language Incentive Program

The Foreign Language Incentive Program (FLIP), which began in November 1982, provides monetary incentives to civilian cryptologic personnel to acquire or retain language skills needed by the Agency. This program is restricted to languages for which NSA has an operational need or which have been designated as Class I or II languages. No one can receive these incentives solely for learning a foreign language.
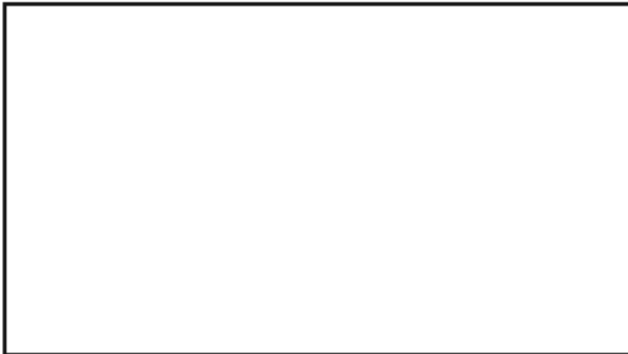
A FLIP position is one requiring the use of foreign language(s), and for which the Career Occupational Specialty Code (COSC), civilian grade, job number and language(s) have been certified as eligible. Civilian employees must be assigned to established FLIP positions in order to receive this incentive pay. FLIP positions

are certified by the individual's supervisor, and include three levels of proficiency:

FLIP is pro-rated for employees in a part-time pay status.

The Family Language Training Program

I am including the Family Language Training Program as a potential source of future linguists, though it was not designed for that purpose. It was established to provide language training for family members of both civilian and military cryptologic personnel assigned to representational duties outside the United States. Training is provided on a voluntary basis, is directly related to the assignment, and may be performed in anticipation of assignment outside the United States.

Family members who are eligible for this program are designated by the DDA in conjunction with the Deputy Director for Plans and Policy and the DDO. The ADT is to be notified of qualified applicants sufficiently in advance of their assignment so that training may be conducted within the United States. Training also may be performed outside the U.S., but only for family members who will be remaining on assignment for a reasonable period following the training. The DDA is also responsible for programming the funds and personnel requirements for this program.

Eligibility is determined by M31 (overseas personnel) and sometimes G Group for country desk positions. This training is done externally at various contractors, depending on language, such as Berlitz, Foreign Service Institute, Language Learning Enterprises, etc.

Because it is limited to family members of personnel representing the Agency at field positions, it is a little known, little used Agency program.

EVALUATION AND RECOMMENDATIONS

These programs offer Agency employees incentives in the form of post-retirement income and training as in the case of the CLRP, additional monetary and training incentives, as

P.L. 86-36
EO 1.4.(c)
2nd Issue 1988* CRYPTOLOG * page 3
CONFIDENTIAL
HANDLE VIA COMINT CHANNELS ONLY
P.L. 86-36

in the case of FLIP, and exposure to language training for family members going to field sites, as in the case of the FTLP.

Each program provides an incentive to pursue specific language capability, although FLIP seems to be more aggressively pursued by linguists than the other programs. The main reasons for this seems to be that it is an ongoing program with wide Agency exposure, offers immediate monetary incentives, and experiences a large increase in the number of participants each year.

According to the outgoing FLIP coordinator, the problems with FLIP are minimal considering the size of the program. Because of FLIP it has become much more important to have positions classified properly, to have reassignments and details done on a timely basis, and for the panels to enter certification records into the system promptly.

Beginning in 1986 a "trailer card" has been distributed to FLIP recipients to remind them that they share in the responsibility for accurate payment of the FLIP bonus. FLIP also requires semi-annual certification by supervisors that personnel receiving FLIP are using the language as part of their duties. This was first done in June 1986 and will be updated every six months.

The CLRP is an excellent means of retaining capability in those languages which are under strength in the Agency. It enables the Agency to draw on experienced personnel in emergency situations. However, although well organized and well thought of by the Agency and its members, the CLRP seems to have run out of gas when it comes to the refresher training that is a requirement of the program. Unless this training is made available, how long can we expect those participating to maintain their interest and their language proficiency?

M3J is still waiting for G Group to prepare the training package for people who have been in the program long enough to require such training. Meanwhile, the G Language Coordinator is developing a language maintenance package that will be applicable not only to the CLRP, but to FLIP maintenance as well. The CLRP will then be assured of having capable linguists in reserve.

Some problems concerning FLIP remain. For instance, there are currently 221 overrides that must be worked manually. This is due to existing qualifiers that are not recognized by the current computer program for payroll. More refined programming should eliminate the need for so many overrides.
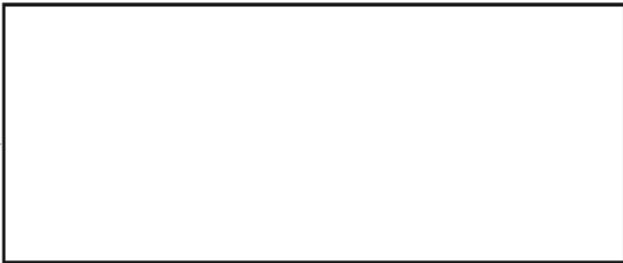
A language committee that has studied this problem has submitted its findings to M37. In June 1986, M37 responded with a rewrite of this COSC. Eventually a change to the Career Service Occupational Handbook and an amendment to the PML on FLIP will be issued and this problem should be resolved.

In the case of the FLTP, although this program was established along with other language and language-related programs pursuant to Section 10 of the National Security Act of 1959, it seems that it was never as fully developed or utilized as other programs. I found that most people were either not aware of its existence or had no knowledge of its ever being used; some were aware that such training was provided for family members going to field sites. Moreover, it is restricted to higher grade levels. Obviously it needs a lot more exposure in order to be of any real benefit, as it does not provide the Agency with a noticeable "return on the dollar" as the other two programs do.

I was left with the question of the long-term benefit to the Agency of this program besides the immediate benefit of having our overseas personnel acquainted with the language of their field site. I believe that it is the potential for second generation Agency family members to develop into linguists as the result of having their interest in a particular language piqued during an overseas tour with their families. This interest could then result in becoming future Agency employees and linguists.

In summary, the Agency has addressed the problem of acquiring and maintaining necessary language capability through the institution of programs such as those addressed in this paper. Some are more effective than others, and some

DOCID: 4019715

need to be focused more closely if they are to achieve what they were initially designed to accomplish.

I strongly recommend that, as soon as it is feasible, a Regulation or PMM Chapter be published as a comprehensive directive for FLIP. To date the only directives existing are PMLs, and considering the magnitude of FLIP,

a comprehensive directive warrants a high priority.

I believe that with these programs and improvements on them the Agency has taken a few first positive steps to correct the chronic problem of being unable to maintain a sufficient number of skilled linguists. I believe that they will in time alleviate the situation. And one program, FLIP, may well serve as an encouragement to linguists to remain in the field.

NOT CRASHING THE SYSTEM

I read with interest and some nostalgia [   ] article in the 1st Issue 1988 of CRYPTOLOG titled "Crashing the System." I helped develop and later managed the RYE system that was mentioned in the article. Now I am involved in computer security matters. For these reasons I cannot resist setting the record straight and making an important point at the same time.

RYE was a transaction processing system which used a priority scheme for scheduling tasks. (I do not believe that the term "transaction processing" was invented in RYE's lifetime.) The priorities ranged from a low of 0 to a high of 7. All RYE executive and operating system software was written by NSA personnel in assembly language. Carol correctly states that RYE used a "greater-than-or-equal-to" instruction to test for priority 7. Since all alphabetic characters were numerically higher than all digits, when she input the letter "B" it was interpreted as a "7."

Sorry, Carol, you did not crash RYE; at worse, you aborted a task so that yours could load. Priorities 0-5 were valued in ascending order of importance. Priority 6 blocked lower priorites from loading. Priority 7 was for "critical" tasks (but not reserved for the Director) and would load immediately even if it had to abort, then later restart, a task. To preserve the sanity of our users, we arranged it so that

[   ] *T03*

certain tasks like file maintainance could not be aborted. We did not want to leave a user with an unthreaded file.

RYE had extensive security and management features well before its time. Its on-line audit trails and analysis tools were valuable both for security and for functional evaluation. When people used the system, they left a "footprint" which we could use to re-create their actions. We could also evaluate every action of the system as it affected reliability and performance. Using these tools, we constantly "tweaked" the system to obtain maximum functionality. When Carol input her priority 7 tasks it resulted in an immediate entry on the operator's console. Analysis of the audit trail identified her as the perpetrator and told us her name, organization, telephone number, room number, and the location of her input terminal. As she pointed out in her article, we called her within one hour.
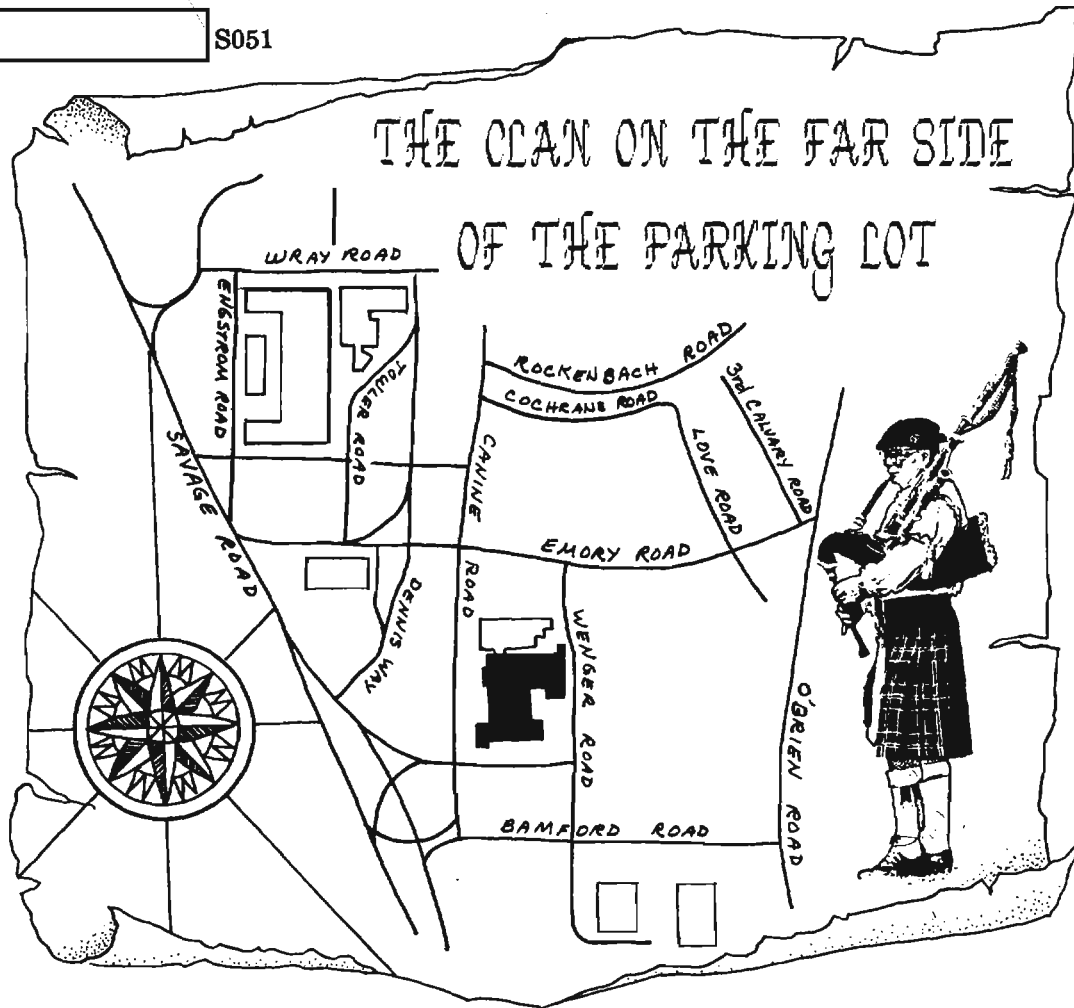
A key point to note here is the value of well-constructed on-line audit trails and analysis tools to support both security and management. ☐

P.L. 86-36

S051

THE CLAN ON THE FAR SIDE OF THE PARKING LOT

P.L. 86-36

(U) Over yonder, a couple of hundred yards southeast of the Main Building, lies a complex unexplored and unknown to a majority of NSA employees. Hidden in recesses of the edifice known as Operations Building 3 lurks the INFOSEC clan. (Pervasive rumors indicate the clan is spreading to the hinterlands of Parkway Center, Friendship, and Airport Square as grazing space lessens at Ops 3.) Rather than continue to let the strange inhabitants known as INFOSECers dwell forever in anonymity, let us take a guided tour to learn their customs, organization, and how they contribute to the security of their nation under the great chief, DIRNSA.

CLAN MEMBERS

~~(C)~~ The clan consists of [   ] including engineers, mathematicians, liberal (and conservative) artisans, technicians, computerers, business administrators, skilled craftsmen and print producers, as well as clan administrators, clerics and assorted shamans and wonder workers. The clan labors under the direction of Chief "Tall Tree" [   ]

(C) The clan is about 67% male and 33% female with an average age of 34. The average INFOSECer has 15 years of schooling, has been with the clan for ten years and has attained the tribal status of GG-10.3. At last count, 200 members of the clan have been initiated into the esteemed cult of "professionalized INFOSECers" wherein they have accrued rights and privileges not available to non-professionalized members.

TRIBAL OBJECTIVES

(U) The clan's mission is to ensure the secrecy and security of information transmitted or processed electrically among all of the members of the nation of which they are part. (An interesting sidelight to this objective is the perception among the INFOSECers that this mission is "the other side of the coin" and helps to support the objectives of a neighboring clan,

the SIGINTers. In fact, this perception is so pervasive it has been said in legend that the two tribes sprang from the same origins and in fact, neither could exist without the cooperation and knowledge provided by the other.)

CLAN ORGANIZATION

(U) Though all serve the same master, there are several separate, but complementary, sub-cultures within the clan that labor together to fulfill the great chief's bidding. These sub-clans are known as the "Cs," "Rs," "Ss," "Sos," "Vs," "Xs," "Ys," and "the Fielders."

(FOUO) The Rs (R1 and R5) support the clan in the production of classified microcircuits, and the research, design and development of cryptographic algorithms for use in INFOSEC equipment. A large new building to house the burgeoning R1s is nearing completion on the edges of Ops 3 and will greatly increase the capacity for fabrication of special devices.

(U) The Ss are a diverse lot responsible for INFOSEC assessments, INFOSEC customer and industrial relations, technical security and INFOSEC planning.

(C) The Vs are the INFOSEC program managers who design, develop, procure and field INFOSEC equipments and techniques for the nation. The Vs contracted for the production and development of over [   ] in the past fiscal year.

(U) The Xs are the system security evaluators and standard developers. They delve deeply into the magic arts of cryptomathematics and TEMPEST.

(U) The Ys run the print facility (rumored to be second largest facility, in terms of quantity of printed materials, outside of the Government Printing Office). The Ys also provide a wide variety of INFOSEC support services to V and C programs and run the INFOSEC computer system complex. The Ys provide INFOSEC keying material (free of charge) to all validated customers, and also print many of the SIGINTer documents.

(U) The Sos provide the management support for the clan and are responsible for administration, finance, policy and doctrine, and INFOSEC international relations.

(U) The Cs are the newest of the groups in the clan and reside at Airport Square 11. (It is rumored that a new building for them is under construction.) The Cs, in addition to supporting the clan internally, also function as the National Computer Security Center, responsible for developing standards and evaluating applications of commercial computer products for the protection of classified information.

(FOUO) The Fielders represent the clan around the world. There are full-time INFOSEC fielders located at NCPAC, NCEUR, NCR DEF, [   ] SUSLO CHELT, NCR SAC, [   ] and NCR SOUTH. There are also INFOSEC fielders at the Treasury Department, JCS, WHCA, NNBIS, U.S. Trade Representative, and GSA.

WHAT THE INFOSECERS DO

(U) Meeting the INFOSEC objective of protecting sensitive information is, in my opinion, as much an art as a science, so it is very difficult to describe how it is done. To make it clearer to those not acquainted with the INFOSEC methodology, here is a generalized example:

(FOUO) An INFOSEC need (i.e., a need to protect national security information that must be transmitted or processed electrically) is established by a customer. The recognition of a need may be initiated by the customer or may be the result of an INFOSEC assessment (an analysis of threats vs. vulnerabilities) by the clan done at the request of the customer's organization. Examples of types of needs most commonly seen by the clan are needs to trust a computer or ADP system to limit file access, needs to protect a new communications system from exploitation, and needs to securely intercommunicate with allies. Before the need is then validated through tribal and national management, it must be clearly elucidated and fleshed out between the customer and a customer account executive to determine if it can be satisfied through an existing INFOSEC equipment or technique, or if a new development is required. Regrettably, in some cases, the clan lacks the resources to solve the competing needs of all its clientele.

(U) If the need can be satisfied through application of an existing INFOSEC equipment or technique, the customer is provided with procurement information, costs, delivery dates,

and technical parameters of the selected equipment or technique; the customer is also provided with assistance for ensuring that the integration of the technique or equipment within a given application is sound. The customer is asked to provide (and help is given to him) in formulating his concept of operations, key management and key requirements, maintenance concept, installation and fielding plans, and training. The customer is consulted in the development of system and equipment doctrine and kept advised of equipment modifications that may be necessary during the life of the equipment. Assistance and customer support is provided by the clan throughout the life of the requirement.

(U) When the customer's need cannot be satisfied by an existing equipment or technique, the clan may undertake development. The process described above is front-ended by identification of funding, task prioritization establishment of a development plan and milestones, algorithm design or technique development, evaluation, fabrication and contracting. In many cases, a test and evaluation is specified to ensure correct operation in a system.

(U) In both cases the clan must ensure that both the design and implementation of the equipment or technique are sound, that a multitude of security-related considerations are satisfied, that the customer understands INFOSEC policy and doctrine related to the system, and that the customer has the corporate infrastructure necessary to ensure that INFOSEC is, in fact, being obtained.

WHERE THE CLAN IS HEADED

(U) The business of the clan is constantly expanding as more and more of its customers recognize the need for INFOSEC and as telecommunications grow and computers proliferate. The clan has found that closer relationships with industry can provide help and ensure that INFOSEC needs are satisfied by drawing upon the expertise of industry. The clan has established a very close working relationship with the computer industry and is encouraging the use of their resources in developing computer security techniques and products. It is likewise working with the carriers of communications to ensure that INFOSEC needs are considered in the development of switching and transmission systems.

CONCLUSION

(U) From this brief sojourn we have learned that the INFOSECers are not so strange after all. Some of you may even know them, ride in car pools with them, and associate with them. We have also concluded that the far side of the parking lot is not so far away and is an integral part of the NSA structure and mission.

AN INVITATION

(FOUO) I was asked by tribal management to dispel the mystery surrounding the clan and to spread the word and invite talented SIGINTers and other personnel to help the clan prosper and meet its objectives. I am convinced that the clan has an active intern program and a program to help on-board INFOSEC personnel join the cult of the professionalized and advance through the organization. As outlined during my tour of the tribal organization, the challenges faced by the clan are unique, interesting, and provide a real sense of satisfaction. The tribal chief has invited all interested NSAers interested in learning more about INFOSEC or in becoming INFOSEC clan members, to contact the INFOSEC Career Panel, H113, 972-2308. □

Solution to NSA-Crostic #66, 1st Issue 1988

Arthur J. Salemme, "A Few Tricks of the Trade (for the Translator of Russian)," NSA Technical Journal, Fall 1966.

If the translator of Russian can maintain the author's original style and can avoid awkward constructions in English, he will be more and more likely to hear the ultimate compliment of the non-linguist, "Why, it doesn't even sound like a translation!"

THE FALSE FRIEND: A True Story

G609

FOR OFFICIAL USE ONLY

BULLETIN BOARD

SUN USERS GROUP

Persons interested in joining a SUN Users group are invited to make themselves known to [   ] R53, FANX III, 968-8845.

UNIX SEMINARS

CRYSCOM is holding monthly brown bag seminars on UNIX in the North Cafeteria in the room behind the glass doors. Interested persons are invited to attend. For a schedule and further information, get in touch with [   ] T335.

MACINTOSH USERS GROUP

Persons interested in forming a Macintosh Users Group are invited to make themselves known to: [   ] R822, FANX II, 968-8807 or 963-1011.

SOURCE OF OUTLINE MAPS WANTED

CRYPTOLOG is seeking a source of high quality reproducible black-and-white outline maps. Geographic now stocks only colored maps which do not reproduce well. Also, they are cluttered with irrelevant information, which makes it impossible for authors to superimpose their own information legibly.

For articles published in CRYPTOLOG we need the kind that is used in schoolrooms, showing only rivers, or roads, or principal cities, or national boundaries, etc., that children fill in for tests. Please note that maps output on a dot-matrix printer are not of acceptable quality. Call the Editor, [   ] 963-1103 or send a note to her at P1, HQS

SOFTWARE ACQUISITION: A REFORM IN NEED OF REFORM

P.L. 86-36

[_____] T35
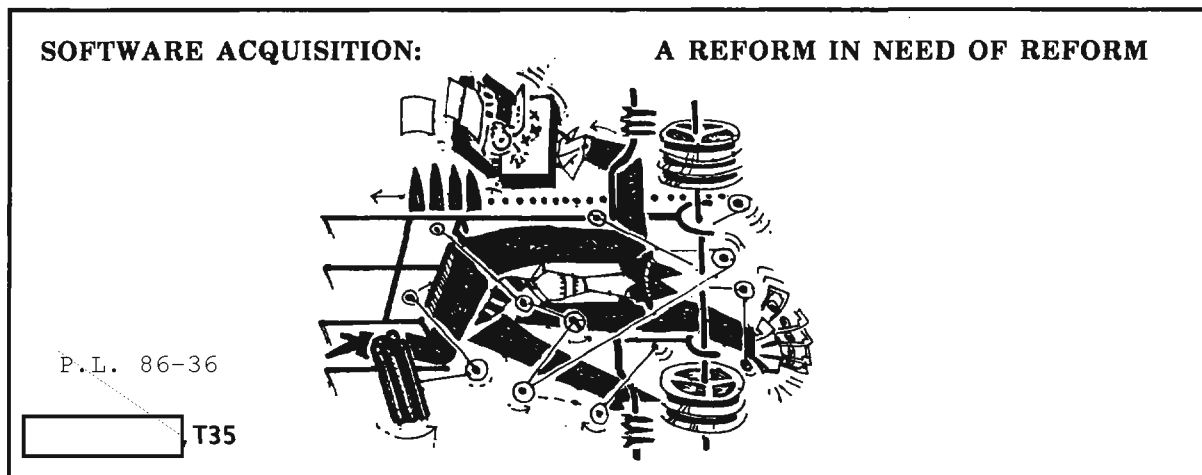
In the fifties and sixties, software development had been by the seat of the pants – get the job done as quickly as possible, documenting afterwards if time permitted. Then, in the seventies, fueled by anxieties over the growing costs of software maintenance, and virtually mandated by reports from the Director's Scientific Advisory Board, software development underwent drastic reform.

The reform had its most dramatic impact on the methodology of developing software. It came to be known as "software acquisition," and the pendulum swung virtually 180 degrees from seat-of-the-pants to a series of formal, discrete, sequential steps. These consisted of: gathering all the requirements, reviewing and freezing them; drafting a preliminary design and reviewing it; detailing the design, reviewing, and documenting each step of the way; coding, unit testing, integrating, and finally, bowing to the few customers who outlived the process.

The reform affected both policy and procedures. Some of the resulting policy measures have been beneficial, such as employing higher-level language in the place of assembly language and employing commercially available off-the-shelf software where feasible. And undeniably, the Agency had been paying (and is still paying) a high price to maintain software that had been developed quick-and-dirty and that was never cleaned up. Some correction was needed to obtain cleaner and more maintainable software.

In recent years, a larger portion of the Agency's software has been developed under contract, and its effect on the cost of that software

should not go unmentioned. In the past, formal deliverables had been required as a part of any software contract, but now, contractors are required to adhere to the Agency's formal software acquisition methodology.

Incontrovertibly, contractor-developed software comes at a much higher cost than in-house developed software – say a cost factor of two or three per man-year. Since the cost of employing the current methodology adds its own overhead factor – in my estimation perhaps a factor of two or three – software developed out-of-house is costing the Agency perhaps four to nine times what it might otherwise cost.

I acknowledge that the software being delivered today is cleaner and easier to maintain than in the past, but I contend that in terms of costs expended and value subtracted, the trade-off is unacceptable. The cost of the cure has been more than that of the sickness. Specifically, the practices which have evolved in the quest of developing maintainable software are outrageously costly in up-front manpower and time, and are doing grievous harm to the Agency's ability to deliver a timely, useful, product. And I firmly believe that it is possible to acquire clean and maintainable software at a much lower cost.

It should be noted that many who extoll the benefits of the new methodology are from the private sector or academia with an axe to grind: people and organizations who have been enriched by it, such as contractors, course givers, and textbook authors. I can recall no CISI speaker who advocated this methodology who did not have something to gain by so

doing. Prolonging projects is meat and drink to these people. No contractor would welcome a change in Agency methodology that halved rather than doubled the duration of its software contracts.

Moreover, the delivered product is often apt to be not quite right owing to inevitable changes in the requirements. In sum, today's software acquisition process subtracts timeliness and responsiveness from the delivered product and adds additional costs. My observations lead me to believe:

> that today's software acquisition methodology is having a debilitating affect on the Agency's ability to deliver timely, functional software;

> that Agency dp customers have recognized for sometime that the process isn't working;

> that Agency finance people have recognized for some time that software costs are spiraling, but without obvious improvement in quality, timeliness, or customer satisfaction;

> that Office and Group Chiefs are experiencing a sense of malaise over a growing inability to respond to operational challenges with timeliness except when a quick-response situation is decreed.

Nevertheless – perhaps because of the lulling affect of academicians and consultants who are either unaware or unconcerned about the needs of the Agency to expedite the delivery of software – Agency software acquisition methodology has continued to go unchallenged.

FALLACIOUS PREMISES

Today's software acquisition methodology seems to be based on a number of fallacious premises. One is that more work makes for a better ultimate system. It is a fallacy because the "more work" is not technical but bureaucratic. More documentation is required, more inspections, more reviews, more workers, more coordinators, more and larger teams, and so on. I note that:

> bureaucratization is seldom salutary;

> the more people involved in an effort, the more overhead will be involved in coordinating that effort;

> individual accomplishment, motivation, and morale are reduced rather than raised

when each person is asked to play a lesser part in a large group effort.

The major fallacy is bureaucratic formality which tends to treat system development as a closed set of well-documented sequential steps rather than as an interactive process. Consider, for example, how the methodology calls for an extensive up-front effort to identify and document every last requirement at the outset. Since requirements are seldom static, and seldom clearly and accurately known at the start, this is effort ill-spent.

I believe that it is better to gather the major and obvious requirements, and accumulate additional requirements as the project progresses, since the development of a system should be interactive rather than sequential in order to expedite the development and to ensure the fidelity of the product. The charge of the team should not be "figure out the totality of the user's needs, design a way to do it, document it, then do it." Rather, the philosophy of the development team should be "determine the types of services the user needs, arrive at or develop general software tools to provide them, begin prototyping and interact with the customer until his needs have been met." Documentation should be kept to a minimum until some degree of certainty is present.

Aside from fostering an improper sense of sequentiality, formality in itself imposes a drag on project development to the extent that it inhibits rather than encourages exploiting and integrating the knowledge gained in the systems development process. New or newly-perceived requirements or methods must be filtered through a formal, coordinated, impact-gathering process. Enhancements being thus discouraged, the resultant software product is often bereft of what was learned, and represents the needs and services as they were understood only at the inception of the pr ject. As a result, the long-awaited system is apt to disappoint when it finally is delivered.

In the past, software developed ad hoc, though imperfect, had the redeeming merit of giving the user the function he needed in a timely fashion. Today's formality discourages ad hoc enhancements, and serves only to elongate projects.

Another fallacy is that software designers and developers cannot satisfactorily find

DOCID: 4019715

and fix their own mistakes. Admittedly, in earlier days, programming was "by gosh and by golly," in part because it was a new and little understood endeavor. But today's software developers are far better prepared than their predecessors to analyze, design, implement, test, and document. Most of the Agency's newly hired programmers have a degree in computer science (which consists of formalized information gained from the experience of those pioneers in the early days of programming) and so their technical knowledge surpasses that of their predecessors.

Today's methodology – which calls for inspections, walk-thrus, independent test teams, and odious levels of documentation – can only serve to stifle these new hires. I find absurd the notion expressed in the literature that it takes three or four peers to inspect code or design, and that it takes an independent test team to test an implementation team's software. This notion is absurd both in terms of costs and the implied denigration of the technicians. Contemporary developers, given their education and background, require less documentation than did their predecessors and find today's required documentation stultifying to prepare and time-consuming to maintain, and obfuscatory as well, precisely because there is so much of it.

One of life's self-fulfilling prophesies is that when one expects less of people than they are capable of, they deliver accordingly. I see that Agency software acquisition methodology is having the undesirable effect of demotivating its workforce, in flagrant disregard of the respected management writings and teachings of Maislow, Herzberg, and Argyris which are diligently taught by our own Training School.

THE BETTER WAY

Consider the ingredients which are critical to a sound, successful software development:

▸ *A simple design* accepts the premise that the full set of requirements is not knowable from the start, anticipates that there will be changes to the requirements as they were initially stated, and tends to lower the cost per change. A simple design also reduces the learning curve of newly-acquired personnel.

▸ *Prototyping with user-involvement* enables the project to be started quickly, with the

understanding that lessons will be learned rapidly, and that both the customer and the development team will increase their knowledge of the system requirements during the development process.

▸ *Incremental development* assures the customer earliest possible delivery wherever possible, and enables mistakes to be observed and repaired at the earliest opportunity. Turnkey development is risky at best, and is devoutly to be avoided in all but the direst of circumstances.

▸ *A small tightly-organized do-it-all team operating with minimal bureaucratic formality* has the advantage of productivity, high-morale, rapid development, and a high degree of individual responsibility.

▸ *Minimal bureaucratic formality* is a controversial yet key element in the equation. The drag in today's methodology is the amount of documentation which must be generated, and ultimately updated if a change is accepted. It is better to use minimal adequate informal documentation while development is fluid, and to encourage fluidity so as to respond dynamically to new requirements with minimum cost and schedule risk.

An interactive system development effort which involves a small, cohesive design-development team, unburdened by formality, and interacting with the customer on a continuing basis results in:

▸ a product whose risk of disappointing the customer is minimal, and whose initial delivery to the customer is rapid;

▸ a process which rapidly assimilates knowledge gained into the developing product;

▸ a team whose performance is characterized by a high degree of esprit de corps, individual responsibility on the part of each member, and productivity.

While the concept of back-loading rather than front-loading documentation is admittedly controversial, the advantages of a small-team approach are widely accepted. However, many people believe that a small-team approach is inappropriate for any but a small project. This assertion is preposterous. The mistake all too often made is to declare a project "large." If a project is large, it should be broken into

inappropriate for any but a small project. This assertion is preposterous. The mistake all too often made is to declare a project "large." If a project is large, it should be broken into smaller projects. Diners do this when they are eating a steak; savvy managers do this when they organize to solve problems; and the principle is no less true for large software undertakings.

Despite a long history of success in developing smaller systems using a flexible methodology, the Agency has suffered great difficulty in developing large software systems using today's software acquisition methodology. To my mind, the corollary that follows is that large software systems should not be "developed," but rather "coordinated" as a series of small-team minimal-formality efforts. Of course, the interfaces amongst the teams must be clearly defined, and the coordinator must do his job skillfully.

SUMMARY

I find today's software acquisition methodology labor-intensive, costly, and cumbersome, and undercutting the Agency's ability to deliver large software efforts on a timely basis. While the software delivered is value-added to the extent that it is more maintainable than in the past, it is also value-subtracted in terms of its lack of timeliness and responsiveness to the customer. Ancillary drawbacks of the methodology are its inflationary effect on already expensive contracted software, and its demotivating affect upon the workforce. The costs seem to outweigh the benefits by far. A review of the methodology is sorely called for.

An alternative methodology, suggested by the Agency's history of success in quick-response efforts, is to employ small teams which are less formal and more flexible, which emphasize the importance of individual accomplishment, and which are in concert with Agency objectives in productivity and excellence. Extending small-team methodology to the development of large systems requires that large projects be divided into and skillfully coordinated as smaller efforts of a size appropriate to a small team of developers.

Let those readers who feel that the Agency's software acquisition methodology is successful accept my challenge to support a disciplined review and re-evaluation of this methodology. Let those who find agreement with the

contentions expressed here do the same. Nobody wishes a return to the transgressions of "seat-of-the-pants" software development or the repeal of software reform, but the pendulum's full swing appears to be imposing an unacceptable burden on this Agency, and the reform itself is in need of review and reform. □

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

in re LACONIC

_____, DDO/ACAO

P.L. 86-36

Lately, many classification advisors have received queries concerning the use of the term "LACONIC." Its use is sometimes confusing, and it is often taken to indicate a special clearance or classification. It is not a clearance or classification, but a handling control marking.

LACONIC is a restrictive distribution indicator for certain _____ techniques. It is a handling caveat designed to warn the reader that the accompanying material contains information concerning _____ procedures. It does not require a special clearance, but the reader must have a need to know certain _____ ____ details. In addition, this caveat is designed to deny access to contractors and consultants, therefore the marking "NOCONTRACT" should always accompany it. Both markings are used in order to denote that the material is NOCONTRACT because it reveals _____ techniques.

When marking correspondence containing LACONIC material, the caveat LACONIC-NOCONTRACT should be stamped or typed at the bottom of the page in proximity to the classification. An example of a paragraph portion marking is TSC-LACONIC-NC. LACONIC must be spelled out, not abbreviated, in a portion marking.

The NSA/CSS Classification Guide 58-83 further describes the use of LACONIC. Specific questions concerning its use should be directed to P1, on 963-3957s.

(The above information was adapted from Notes From the BCAO, December, 1987, by Richard Sylvester, B/CAO.)

FOR OFFICIAL USE ONLY

A LESSON IN COMPUTER SECURITY
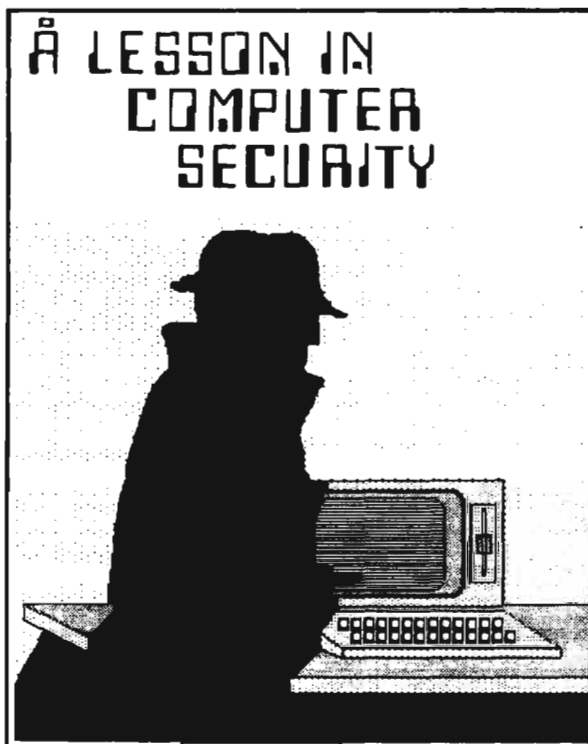
P.L. 86-36   K12

Most of us in Operations don't think much about computer security (COMPUSEC). As an Intelligence Research Intern, I knew next to nothing about it until I worked in X23, the Division responsible for technical computer security evaluations of NSA systems.

Before my tour there, I had assumed that I didn't really *need* to know very much about COMPUSEC. *Somebody* must be taking care of it: "this is NSA, after all. If you can't trust an NSA computer to keep your secrets secret, whom *can* you trust?"

But I learned that in 1986 there were three computer security incidents involving an NSA computer system. The system was DOCKMASTER, an unclassified computer system used by the National Computer Security Center to share COMPUSEC information with contractors. DOCKMASTER is accessible via direct dial-in commercial networks and DoD networks, and can therefore be accessed by a person with a terminal, a phone, a valid user ID, and a password. Although DOCKMASTER is rated as a B2 level system (relatively resistant to penetration), its built-in security features alone were not enough keep out unauthorized users.

In March 1986, someone tricked a DOCKMASTER user into giving passwords over the phone. But after revealing the passwords, the user realized that authorized systems personnel wouldn't need a user's password to get into the system. He called the system administrator, who quickly locked the accounts in question and shut out the would-be penetrator. Do not give your password to anyone!

Another user was denied access in October because his account was already active–in other words, someone had already logged in using his ID and password. The user notified the system administrator, who kicked out the intruder and locked the account. The unauthorized user had previously penetrated a computer system connected to DOCKMASTER. The hacker had apparently implanted a "Trojan horse" which grabbed users' passwords, including the one used to access DOCKMASTER. The hacker logged in over a phone line to the remote host and used the stolen password to log into our system from there. What if the real user had simply assumed, as many would, that there was just a glitch in the system that day?

In still another case, an alert DOCKMASTER user, logging in around mid-November 1986, noticed that he had not been working at the time shown by the system as his previous login time. Like most NSA systems, DOCKMASTER stores each user's login times and, upon login, displays the previous time to the user. Most of us ignore this message, but on this occasion the user noticed that the time displayed by the system had been on a Sunday. The user, who wasn't a shiftworker, immediately reported the discrepancy to the system administrator, who locked the account and prevented further unauthorized access. Subsequent audit checks showed that the intruder had been in the system for a total of two hours and fourteen minutes over several days. That may seem like a short time, but it would have been enough for the intruder to grab over two billion bytes of proprietary information if the owner of the account was authorized access to this data.

Admittedly, there are no classified systems that can be accessed by outsiders as DOCKMASTER was. But consider the possibility of another Pelton. Would you notice if your computer said that you had been logged in during your vacation? □

Data for the Language and Linguistics Section of the Country Reference Books
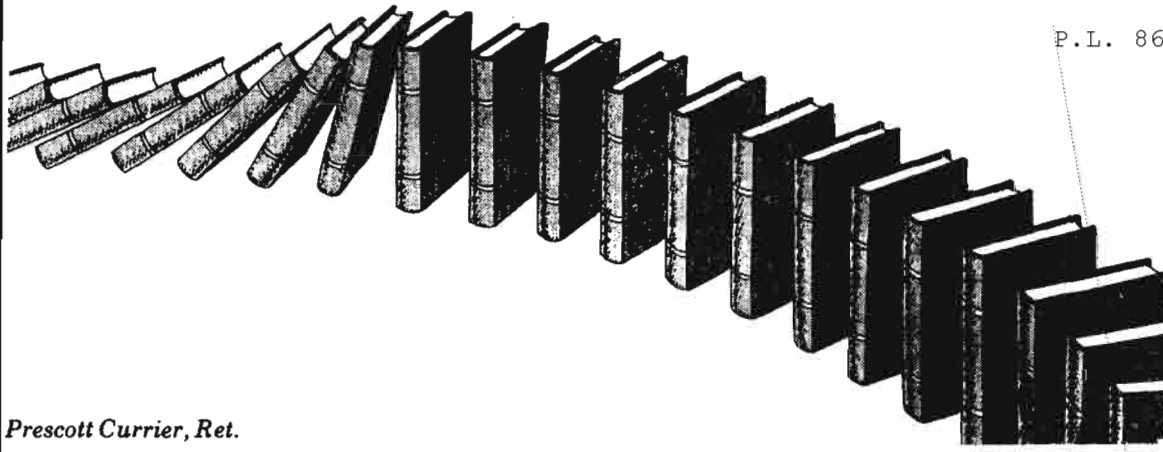
Prescott Currier, Ret.

THIS ARTICLE IS CLASSIFIED CONFIDENTIAL CCO IN ITS ENTIRETY

....
: *This article, originally published in the May 1968* :
: *issue of The Quarterly Review for Linguists, was* :
: *mentioned in the last issue of CRYPTOLOG as a* :
: *model for preparing a language brief. In response* :
: *to many requests for copies we reprint it here.* :
:   :
: *Again we invite linguists to contribute language* :
: *briefs to CRYPTOLOG following this outline or in* :
: *any other format.* :
....

The Country Reference Books are to be a series
of publications designed to provide useful tech-
nical information in ready-reference form on
each of the target countries of interest to NSA.
They will contain data on C/A, T/A, and Lan-
guage, plus an introductory chapter of general
interest material on the country concerned. The
Language and Linguistics Chapter will be
divided into two sections: the first devoted to a
brief description of the characteristics and uses
of the standard language; the second a compen-
dium of cryptanalytically-useful information on
the telegraphic language. A suggested Table of
Contents for the Language and Linguistics
Chapter is as follows:
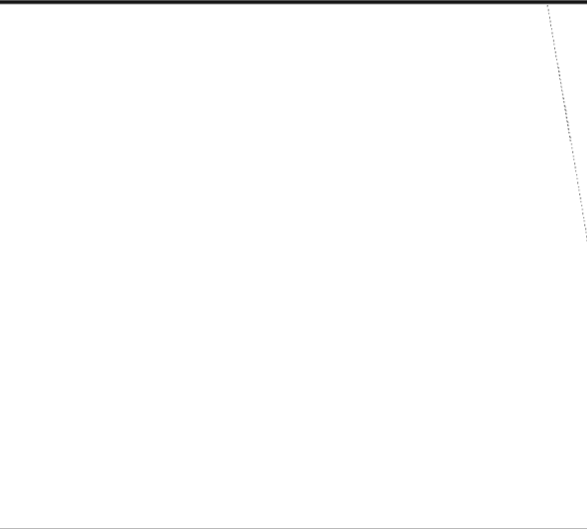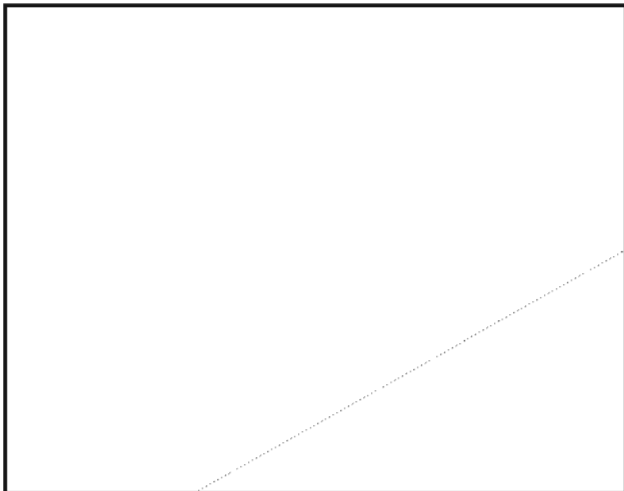
Disappointingly little progress has so far been
made in collecting and compiling the linguistic
data for the Country Reference Books. This is
due largely to a dearth of available talent to
undertake the tedious and time-consuming task
of collecting the rather formidable amount of
data scattered throughout P, and to sort, corre-
late and prepare the material for publication.

To assist in gathering the data already pre-
pared by the various analytic elements for their
own use, it would be very helpful if each ele-
ment could provide P1 with copies of the
cryptolinguistic data now in the hands of their
operational linguists. The data need not be
prepared formally, nor need it be in a pre-
scribed format. The object now is to accumu-
late centrally (in P1) as much operationally
useful language material as now exists but to
do so without imposing too great a burden on
the all-too-few linguists at work on all-too-many
operational problems. If copies cannot be pro-
vided, a simple listing of the material will
suffice. P1 will undertake to get it reproduced.

CONFIDENTIAL
HANDLE VIA COMINT CHANNELS ONLY

A PARTHIAN SHOT

Peter Jenks, Ret.

The author was D/Chief, G, when he wrote this account just before retiring in December 1979. When the paper surfaced during a recent move it was presented to CRYPTOLOG for publication. This is a condensed version.

I am completing some 32 years of work as a cryptanalyst, a career which has taken me from crumbling old IBM listings to something called the Architect for Cryptanalysis; a journey which has taken me through A, B, and G through diagnosis, exploitation, and something called paracryptology; an itinerary in which I have served the cause of cryptanalysis in the most hermetic of compartments and as advocate in the most exposed of locations.

I propose to describe that career briefly, attempting in passing to identify perceptions and convictions which experience later conferred and ratified.

My first experience of the Agency was the training school; in those days (1947) they hired you provisionally first, and cleared you second, and in the interim you passed the time in training school--working your way at your own speed through MIL CRYPT I, II, etc., and doing

it again if you stayed long enough. I was enchanted and somewhat puzzled by the medieval character of both the subject matter and the exposition. The sensation of entering a culture was strong and welcome, if the character of that culture was a little surprising.

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

> *I realized that proving a negative is one of the most difficult tasks facing a cryptanalyst and, in addition, that proving an unwelcome negative carries its own difficulties.*

This was to be one of the most important points in my career both professionally and as an analyst. Marshalling the evidence, securing acceptance of inferential processes, and a clear delineation of the scope and depth of analysis were required. This I did, and got for my pains a promotion and a vastly greater domain of analysis.

Recognition at last! I should not imply that all, or even most, of the foregoing was indebted to me. At least four work centers were

laboring on analogous problems with a common intimation emerging. I fared better than my peers as a result of undisguised ambition, at least in part, but equally because I saw extremely cogent reasons for putting the whole case in writing and acted upon them, if only to deflect the assignment of more resources to a hopeless venture.

My new job entailed, in effect, analytic direction of the work centers mentioned above, the assembly and preparation of branch technical reports, and research. I took all of these things really seriously.

Management at last! I took this, in those days, as a way to extend my reach, to multiply my energies. There were things I felt should be done on a broader scale and in greater depth and now, now I could direct that these things be done. In retrospect, an arrogant and autocratic view, but not totally without merit. At least I knew what I wanted to do.

Publication at last! There was never much doubt in my mind that the world would be better off for my views. By the time I took on this task I was already a prolific writer even if my readership included only my bosses, and the exercise was beginning to pay off for me as an analyst: the articulation of premises, principles of inference, and conclusions has its disciplinary character; the asking of questions makes some demand on oneself as well as others for answers; the enunciation of plans and goals involves similar moral imperatives. Whatever else it did I was in no doubt that this work was making me a better analyst.

Research at last! As it happened, the research I performed here was, yet again, diagnosis but somehow I felt as if my sights had been lifted and as if the goal was something beyond the nearest hill.
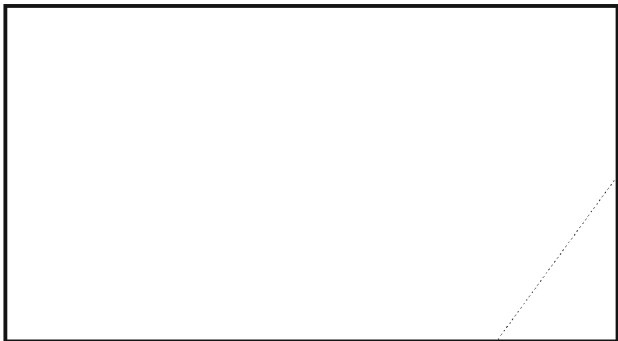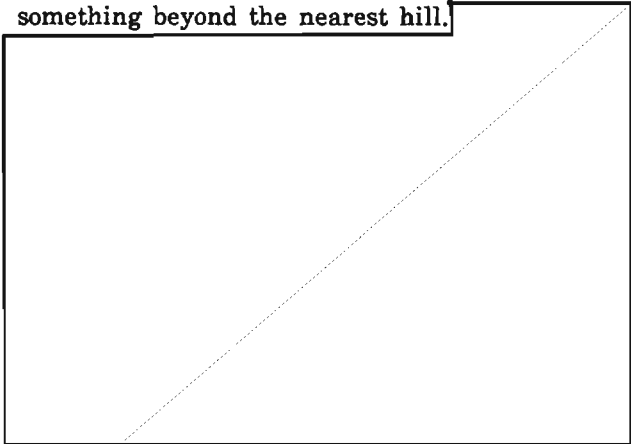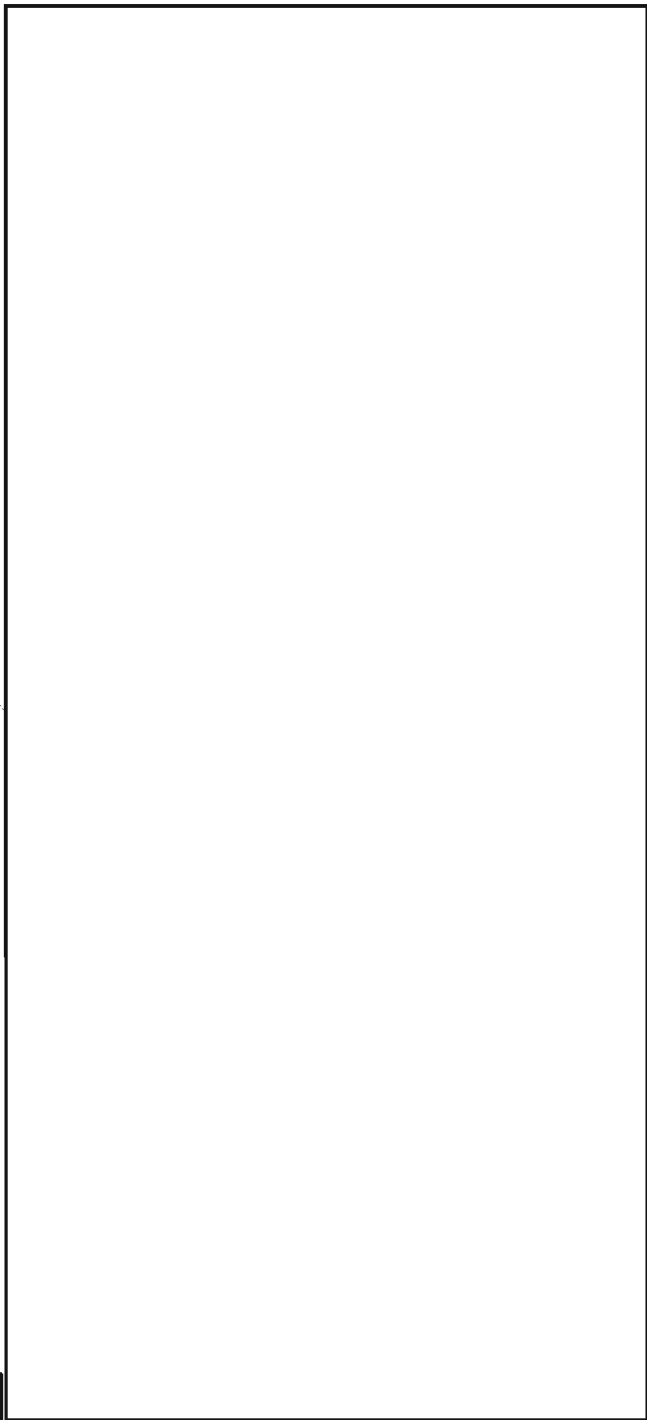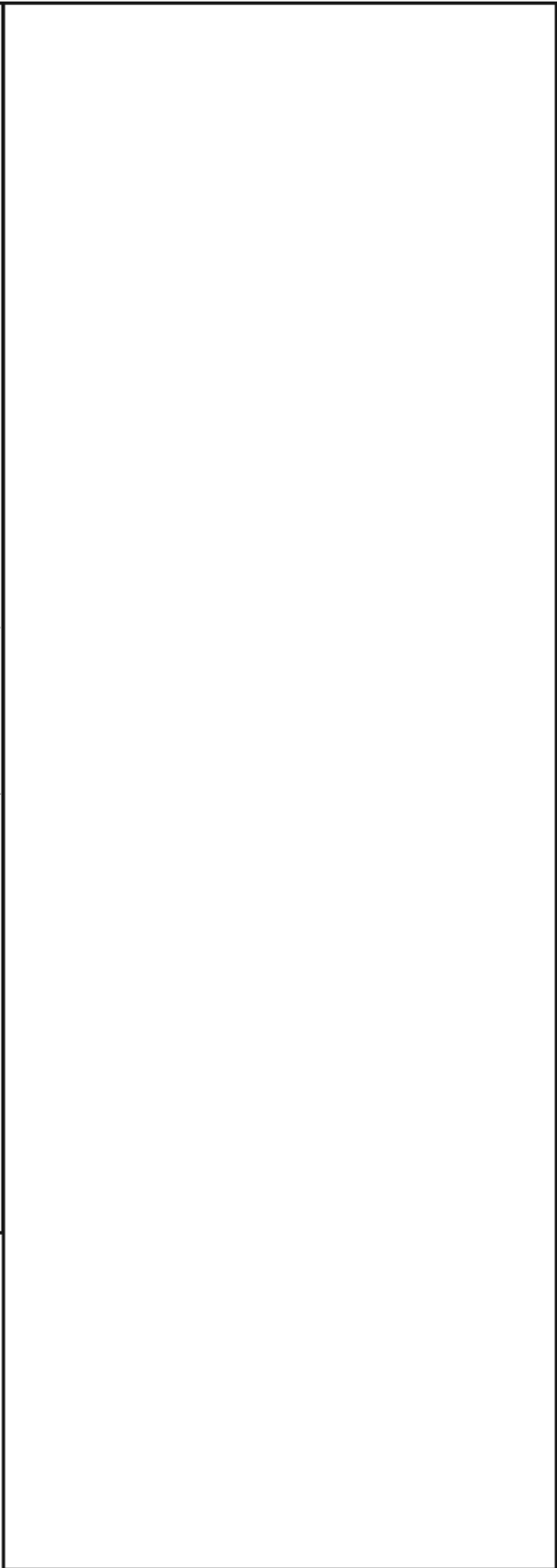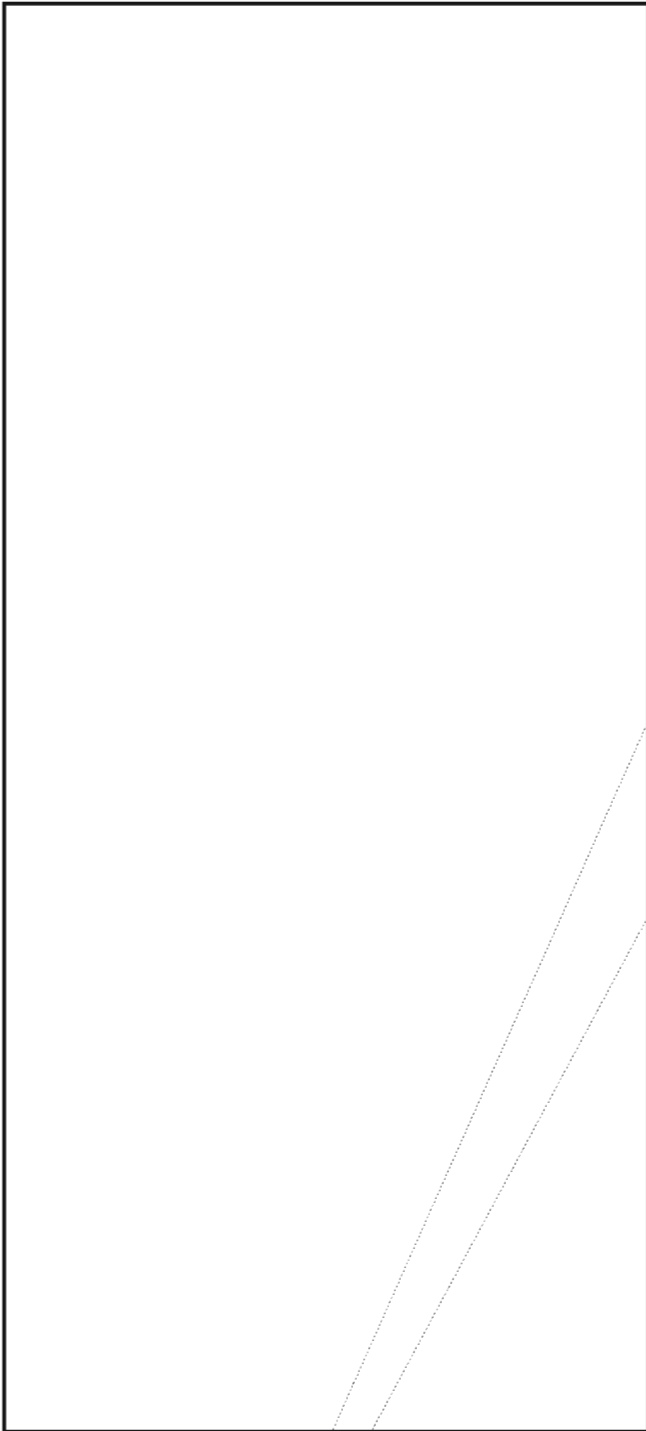
This stupid job and my miserable performance of it obviously qualified me for high office, and midway in that tour I received a very nice offer to be a deputy chief to a chief I much admired (if with some admixture of hostility) and under a group chief who had always intrigued the hell out of me.

At this point I felt there was little left to understand about the target, and indeed that it was time for seniors to make some judgment about the future of the effort. I presented an extended account accordingly of what was known, how it was known, and what, inescapably to me, it implied.

And so I got a new job! The new job involved responsibility for all key analysis, although in practice the mission was directed at one particular target. Primarily on this account the effort was highly compartmented.
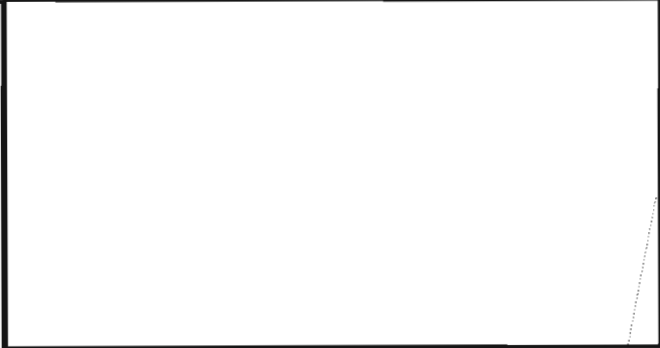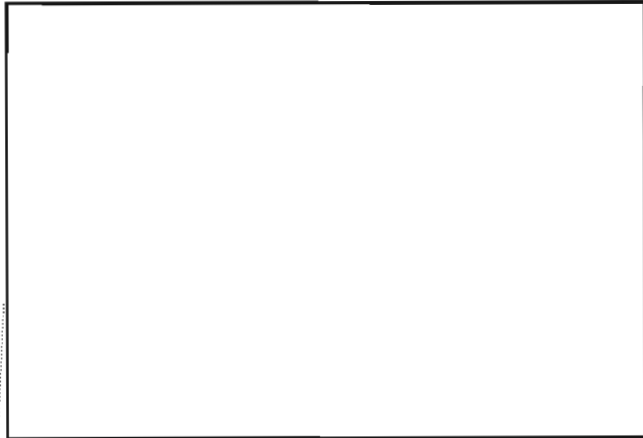
An office at last! With walls and a door. And soon enough, a computer of our own. But more important, although I didn't realize it at the time, was the elite membership of the group and, indeed, the elite character of our bosses. Our little group of twelve was to produce two GS-17's, and one 16, and it was to serve as the seed-bed of a number of enterprises which have since become respectable empires of their own. As is so often the case with such groups, it was independently subordinated, reporting upward by two, rather than one, echelons. In those circumstances, typically, the group writes its own mission, sets its own goals, and monitors its own performance. Given good marching orders and good people it is an arrangement hard to beat.

By the time I took on this task I was already a prolific writer even if my readership included only my bosses, and the exercise was beginning to pay off for me as an analyst: the articulation of premises, principles of inference, and conclusions has its disciplinary character; the asking of questions makes some demand on oneself as well as others for answers; the enunciation of plans and goals involves similar moral imperatives.

It was time once again to assemble all the evidence and draw the inescapable inferences for my bosses. I did this and was sent off to GCHQ as a liaison officer.
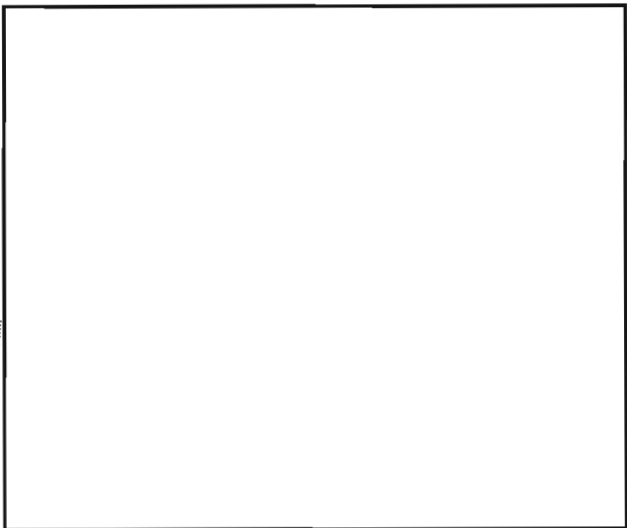
The analytic responsibilities were actually well-timed. By now I felt myself to be possessor of a scientific methodology which worked and which was attuned to me as a person. And at this point I must depart from my plan of not mentioning names. I had resolved not to do so because to give credit to all my bosses, colleagues, and subordinates in just measure would multiply this paper by a factor of ten, and still risk slighting a large number of respected associates and valued friends. Better by far to slight all uniformly and risk the imputation of stealing merit not justly mine. However, there was one NSA figure and one at GCHQ who so decisively shaped me that to ignore them is to tell a fundamental lie. The NSA figure was Art Levenson, my boss in the period just described.

Art, of all my bosses, brought a philosophical turn of mind to his life's job; a recognition that cryptanalysis is a culture with a history and tradition; a sense that cryptanalysis is a science offering an arena for intellectual triumph and artistic Integrity; a concern for the moral and ethical ambiguities which of necessity attach to our work; a high appreciation of, in particular, thought and courage. To a young man whose greatest fear in those days was that he was throwing his life away, there could have been no better boss.

Continuing the slight discursion, there was another cultural force which then and was to continue to shape me. This was the Class of '51. In that year a bunch of extraordinary young mathematicians, hired at once in a deliberate and careful way, and mainly assigned to 206 (later 064), the Agency's training ground and base of operations for the cryptanalytic elite. I was very envious and, in fact, jealous of this crew. I would have welcomed early on an invitation to join 064 but later it became a point of pride to me to not be in it.

Negative influences, though, can have powerful effects and not necessarily bad. Feeling set off from my peers and destined to a different route, I both consciously and unconsciously set out to make the best of that, often as not by a deliberate contrast. This was all very well but a difficulty was about to emerge. Briefly, to be a good liaison officer you need at a minimum two things—a knowledge of the field you will represent, and an old-boy relation with the leaders in that field. I found myself with neither.

I had no experience [   ] or of those who directed it. A series of briefings and a well-filled notebook were not to remedy this. Both the problems and the people swarm in my mind. If ever I was going to

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

have to fake it, the time was now. And so to GCHQ.

I was to find the job detestable but not for the reasons I feared. The job turned out to be an office boy task complemented by supposedly obligatory rounds of party-going. I found that my predecessor had developed an idiotically complex and comprehensive filing system for documents never again referred to, and an equally time-consuming mail distribution and logging system whose chief attribute, as I saw it, was the destination of documents to long-ago abolished organizations. This situation I corrected only to find myself thereafter with nothing to do. Well, as noted above, I didn't know the field [   ] worth a damn so I passed the time mainly by reading the technical reports I was charged with passing to and fro. This proved in the long run to be a very smart thing to do. But I can't say I knew it then.

This stupid job and my miserable performance of it obviously qualified me for high office, and midway in that tour I received a very nice offer to be a deputy office chief to a chief I much admired (if with some admixture of hostility) and under a group chief who had always intrigued the hell out of me. The office, moreover, was engaged in [   ] a field in which now I felt at home and anxious to make a contribution. I was spared by this happy offer the humiliation which characterized the typical overseas tour-- looking for a job, hat in hand. This, plus getting a promotion at much the same time, certainly mitigated an otherwise somewhat depressing tour. I am speaking professionally of course; I and my family loved the non-professional aspects of the tour.

Before leaving the matter of GCHQ I must make a bow in the direction of [   ] I had seen Hugh from the fringes several times in the past decade and there was nobody in my life who had impressed me by half what he did. He had then and continued to have for me the attributes of genius, an almost naive innocence in approaching new problems, all too swiftly followed by profound insight, and an instinct for the jugular insofar as that problem was concerned. A strange mixture of art, scholarship, and science. Not without the defects of his virtues either; impatience, arrogance, irrelevance. This exposure was of some importance to me. I

wanted very much to believe that my chosen field captured and nurtured transcendent intellects, and in Hugh any doubts I had were laid to rest, so back across the ocean.

To some [   ] problems of which I had no first hand experience whatsoever, and analyzed by some 200 people, virtually all strangers to me. I wasn't, nonetheless, alarmed about the problems (I had, after all, read a good bit about them) except in the sense that I seriously doubted that I could make a high technological contribution in such a complex field. At this stage and eminence, such a contribution was, of course, unnecessary but, since the only way I know of earning respect is earning it I felt uneasy. More to the point, I knew that what I would have to do to earn my pay was to make judgments, often as not on insufficient evidence. How to do this with only theoretical knowledge and supported wholly by subordinates unknown to me promised to be a difficult task.

It should be emphasized that the name of the game, here, was solution and exploitation, not diagnosis which was where my most solid experience lay. It seemed to me that the world would survive, at least temporarily, if I didn't know or do what my subordinates knew or did. Then things would go rather better if I learned and did what they didn't.

I should attempt to develop a rather fine generalized picture of what this organization did, where it had been, where it was going, how its internal priorities were arrived at, how it fitted in its environment of support systems, competitors and consumers, how it should be governed, and to what end.

I felt that if I knew that, I would know something no one else did and could turn it to account to earn my pay. □

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

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

COMPUTER
DISPLAY
DEVICES

BY :
P13

P.L. 86-36
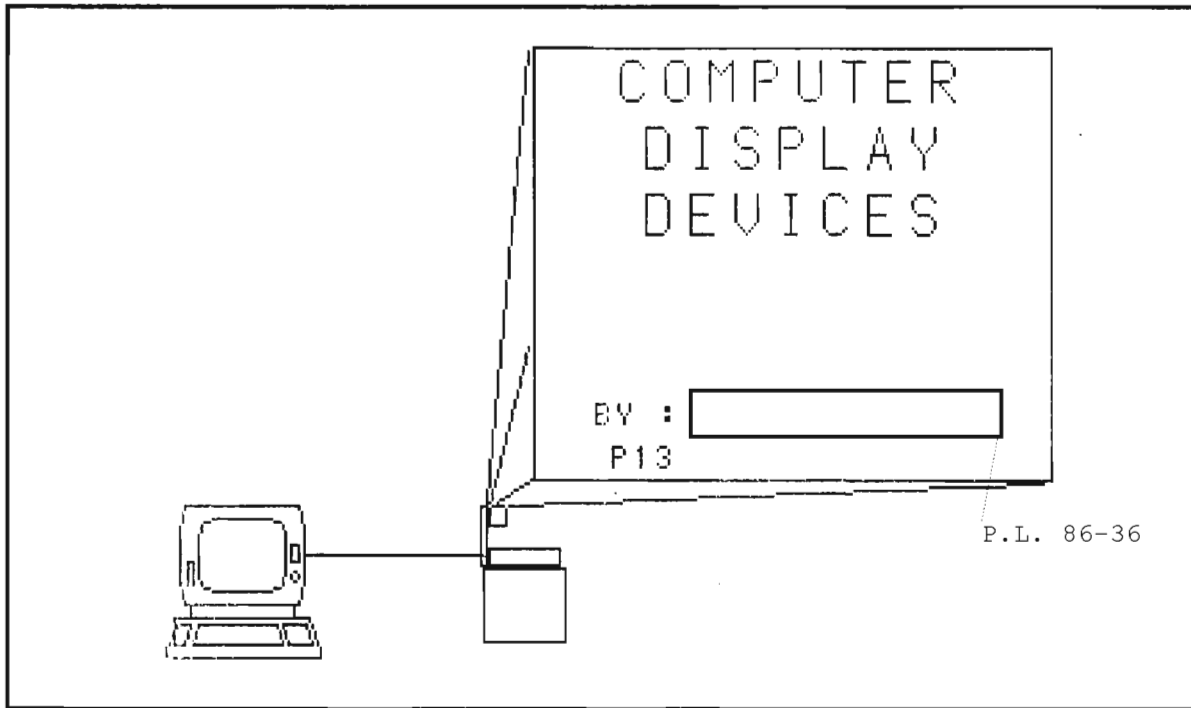
If you have to brief a number of people about some new software, you need to use a data display device, for no more than two people can read what's on a PC monitor at the same time. The device is attached to the computer and projects a screen image onto the wall using an overhead projector.

P13 recently bought one device and obtained another on loan. We bought the **Data Display** by Computer Accessories Corporation at a cost of $1000.00. We borrowed the **Magna Byte II** by Telex Communications Inc., which costs $1500.00. Both displays come with software to capture screen images and to prepare slide shows using the captured images. Following are our observations of the two devices:

The Magna Byte II

▶ has the option of using instructions in English, French, German or Spanish;

▶ displays the screen images in color, not all the same colors as the screen but still impressive;

▶ offers a graphics mode with software to allow for the creation of piecharts, barcharts and text in a medium-resolution graphics mode;

▶ allows you to change slides in the slide presentation through a time interval sequence

you specify or by using a wired hand-held remote control;

▶ requires a controller card which must be installed in a slot in your computer; this limits its portability.

The Data Display

▶ gives a good resolution black and white presentation;

▶ has an optional carrying case for portability.

CONCLUSIONS

Although the Magna Byte II offers color display, a graphics package, and a wired remote control, it has a major disadvantage for us: it is not readily portable. The controller card which must be installed in a slot in the computer tethers the device to the computer and so limits its portability.

We chose the Data Display, which gives a good resolution black and white presentation and is highly portable. P13 created a nice portable presentation package consisting of this device, a Zenith lap-top computer, and a folding overhead projector.

For further information or a demonstration you may call anyone in P13 on 963-3045(s). At present we are in room 2C030, OPS-1. □

TECHNICAL LITERATURE REPORT
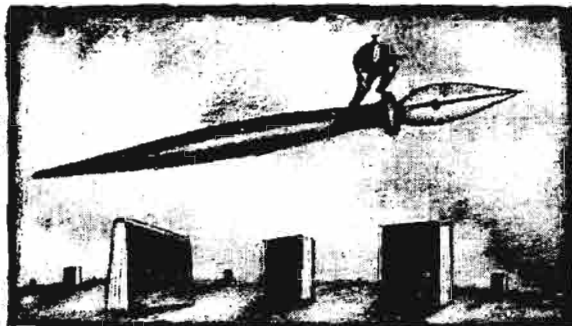
Reported by: David Harris, R51

M. M. Pozzo & T. E. Gray (1987) "An Approach to Containing Computer Viruses," *Computers and Security*, 6, pp. 321-331.

A computer virus lures unsuspecting users into executing it in the course of carrying out an allegedly useful program, while in reality it performs additional functions intended to give unauthorized access to the system or to damage the operation of the system and its contents. For example, recently it was reported in the news that an American corporation fell victim to a Christmas virus. The virus produced a Christmas tree display on a terminal and asked the user to carry out a seemingly innocent action. If he did so, the side-effect was to distribute a similar Christmas tree display to all people to which the user had access. Rapidly, the Christmas virus spread throughout the corporate network, even across the Atlantic. Eventually the network crashed from the communications traffic jam, and the network had to be taken down while operations systematically removed the virus from each and every user's space.

Viruses can modify other programs, perhaps by making them adjoin a copy of the virus itself, thus spreading the virus throughout the computer. The virus, once it has infected a user's software, may be used to give the attacker access to all the user's other files. Further, any third user will become infected if he uses an infected user's software. This paper presents a mechanism for containing the spread of a computer virus by detecting at run-time whether or not an executable statement has been modified since its installation. The detection strategy uses encryption. The method avoids assuming that it is sufficient to prevent modification of executables by unauthorized

users. The authors suggest using public key encryption.

←——————————→

Eliot Marshall (1988) "The Scourge of Computer Viruses," *Science Magazine.*, 240, 8 April 1988, pp. 133-4.

This article appeared in the News and Comment section of *Science Magazine*. Marshall describes the problem, gives some history of computer viruses in the workplace, and talks about efforts to protect against the threat. In general, the article is negative about the role of NSA, concentrating on what it says are our efforts to downplay the problem. Marshall believes that we feel that it is best to give this subject as little publicity as possible so as not to stimulate hackers to develop viruses. He quotes Fred Cohen of the University of Cincinnati as saying "One of the NSA guys told me to my face, 'You're not going to do any research on viruses if we can help it...'." Clearly, Marshall does not agree with this approach. He believes current protections are largely inadequate, and much more research ought to be done. Cohen does concede however, that while the NSA does not announce its plans, "they seem more concerned now because they've got people researching it."

←——————————→

K. Hwang (1987) "Advanced Parallel Processing with Supercomputer Architectures," *Proceedings IEEE*, Oct. 1987, pp. 1348-1379.

This is a rather comprehensive survey of supercomputers and supercomputing. To quote the introductory blurb, it "... presents advanced parallel processing techniques and new hardware/software architectures ... (with) emphasis on vectorization, multitasking, multiprocessing, and distributed computing. Important issues addressed are architectural choices, parallel languages, compiling techniques, resource management, concurrency control, programming environment, parallel algorithms, and performance enhancement methods." It includes an assessment of the potentials of optical and neural technologies, and a survey of available supercomputing hardware.

All in all, anyone with a serious interest in the field would probably want to look over this article. □

On the Lighter Side
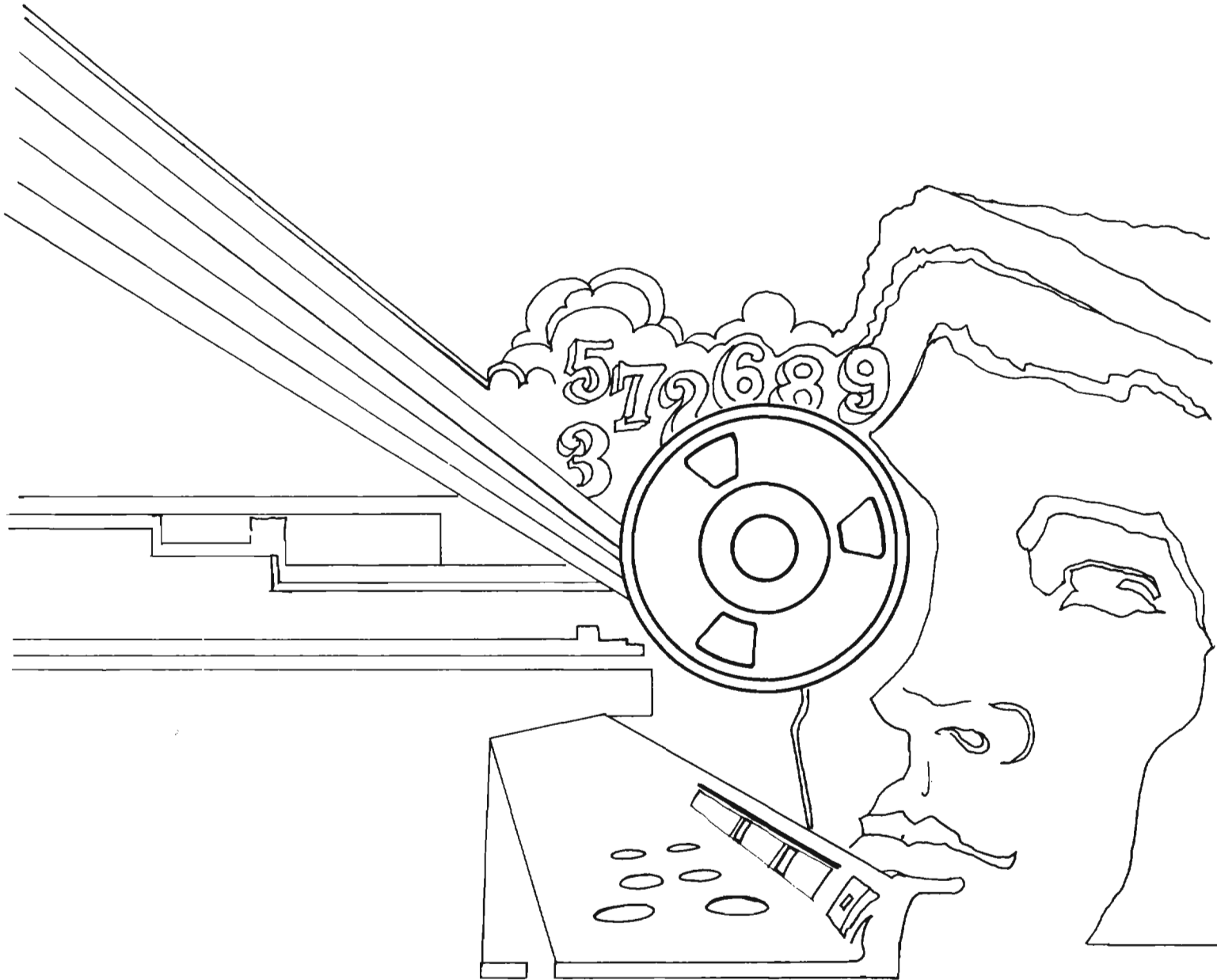
CRYPTO "LOG" PUZZLE

By [   ] *T12*

"Log" is one of many English words with several different meanings. Also, its letters form parts of other words. The following clues define words or phrases that contain "log." How many can you guess?

1. Ridiculously simple -

2. Of or affecting the mind or its working - - - - - - - - - - - -

3. Immovable mass or blockage - - - - - - - - - - - - - - - - -

4. Child's building set -

5. A box in a theater or opera house - - - - - - - - - - - - - - -

6. Mutual help, especially with political programs - - - - - - - -

7. Lacking vitality; sluggish - - - - - - - - - - - - - - - - - -

8. Detailed record of a voyage - - - - - - - - - - - - - - - - - -

9. Systematic list of library books - - - - - - - - - - - - - - -

10. Sound asleep -

11. Slept soundly -

12. Principal Indonesian language of the Phillipines - - - - - - ,

13. Disagreeing, arguing, or quarreling - - - - - - - - - - - - -

14. Reserve or accumulation - - - - - - - - - - - - - - - - - - -

15. Did absolutely nothing -

16. Wood burned at Christmas - - - - - - - - - - - - - - - - - - -

17. Computer using physical quantities to represent numbers - -

18. Abraham Lincon's birthplace - - - - - - - - - - - - - - - - -