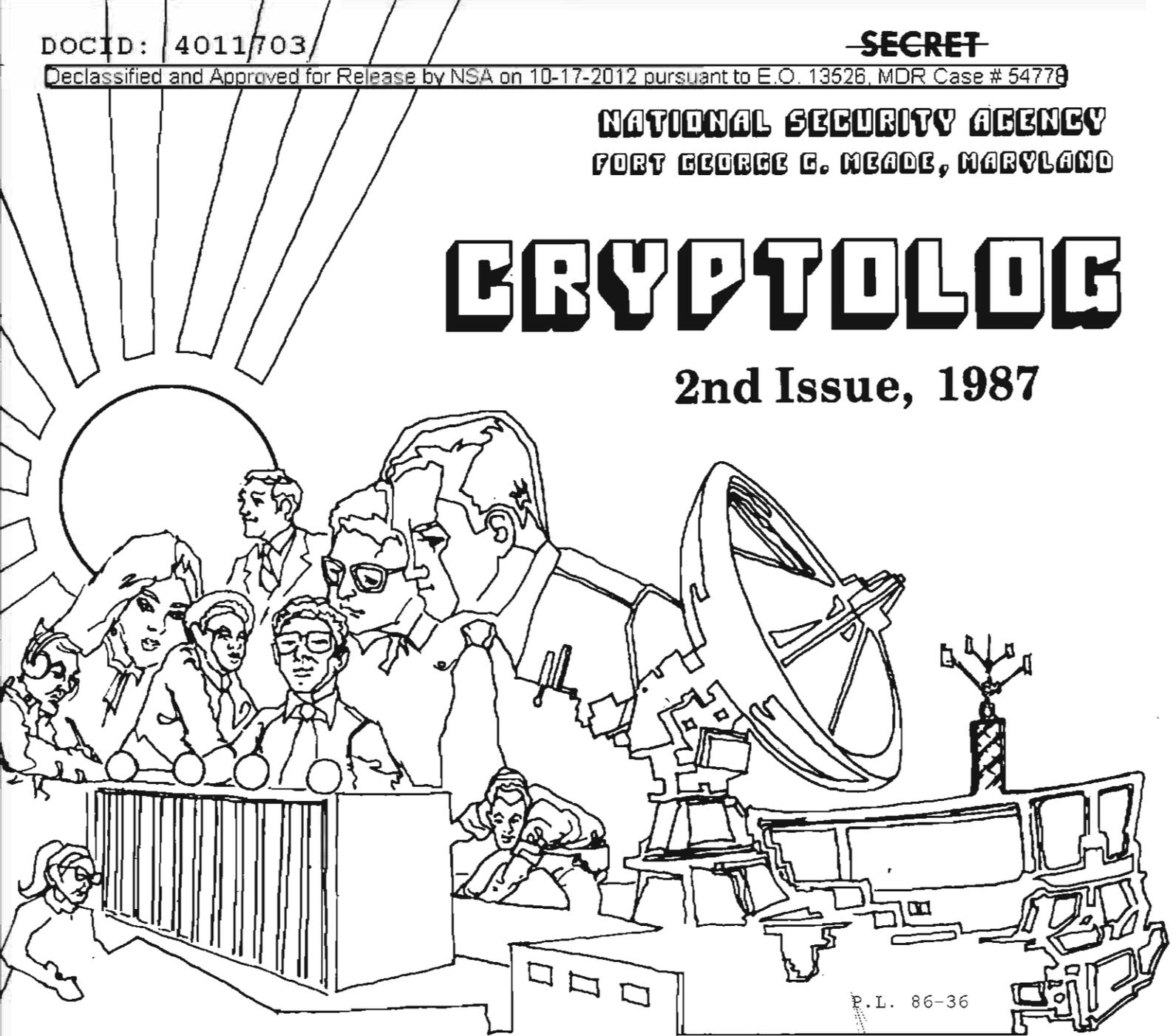


NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

2nd Issue, 1987



P.L. 86-36

THRUST FOUR (U)	[]1
BULLETIN BOARD (U).	[]5
INFORMATION MANAGEMENT FOR THE FUTURE (U)	[]6
FOOD FOR THOUGHT (U).	[]8
MODEM COMMUNICATIONS (U).	Frederick Rodean.9
LETTERS (U)	[]	16
THE RECKONING (U)	[]	17
SOME TIPS ON GETTING PROMOTED, 3rd ed. (U).	[]	19
CONTRIBUTIONS SOLICITED	[]	29
GETTING STARTED	[]	30
GOLDEN OLDIE (U).	[]	31
NSA-CROSTIC No. 64 (U).	[]	32
HOW RUSSIANS VIEW THEIR LEADERS (U).	[]	33

~~NOT RELEASABLE TO CONTRACTORS~~

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

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

P.L. 86-36

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XIV, No. 2 2nd Issue 1987

PUBLISHER [redacted]

BOARD OF EDITORS

- Editor [redacted] (963-1103)
- Collection [redacted] (963-5877)
- Computer Systems [redacted] (963-1103)
- Cryptanalysis [redacted] (963-5238)
- Cryptolinguistics [redacted] (963-1596)
- Index [redacted] (963-5292)
- Information Science [redacted] (963-3456)
- Information Security George F. Jelen (859-1211b)
- Intelligence Research [redacted] (963-3845)
- Language [redacted] (963-3057)
- Mathematics [redacted] (963-5566)
- Puzzles [redacted] (963-6430)
- Science and Technology [redacted] (963-4958)
- Special Research Vera R. Filby (968-8014)
- Traffic Analysis Robert J. Hanyok (963-4351)
- Illustrators [redacted] (963-3057)
- [redacted] (963-6211)

AVE ATQUE VALE

(u)

P.L. 86-36

There's a change in the masthead. [redacted] who was publisher of CRYPTOLOG for six years, has moved to Z. They will benefit. He is taking to the Chief Scientist's Office what he brought to P1 and to CRYPTOLOG: a passion for the arcane arts practiced in this Agency; a concern about documenting current efforts to benefit our successors; an active interest in the storage and retrieval of information; and an enviable skill in expository writing.

Happily, he is not lost to CRYPTOLOG. He has merely become its friend rather than its publisher: almost the first thing he did in Z was to pass on some items for publication, and he has since helped us in other ways.

Good luck, Glenn, on your new assignment. We look forward to our new association with you.

We are most pleased to welcome [redacted] as the new publisher. He comes to us from G4, where they practice esoteric disciplines. He is a natural for CRYPTOLOG, as he is noted for the breadth of his technical knowledge, his championship of passing on the torch, and for his singular gift of explicating highly technical matters to non-specialists. That's what we're all about!

Welcome aboard, Joel

P.L. 86-36

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.

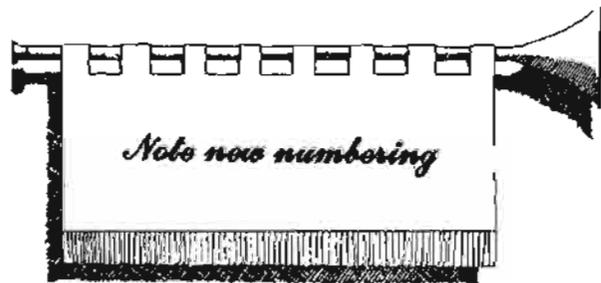
via PLATFORM mail, send to:
cryptlg@bar1c05
(bar-one-c-zero-five)
(note: no 'o')

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.



~~CONFIDENTIAL~~

*The Director's
Thrust #4 (U)*



P.L. 86-36

[Redacted] Z

This article is classified ~~CONFIDENTIAL~~ ~~COO~~ in its entirety

This was the Keynote Address at the 1987 session of the annual seminar series, CA-305, Contemporary Issues in Cryptanalysis. At the time the author was Chief, P1. P.L. 86-36

[Redacted]

The one of most interest to us as cryptanalysts is Thrust #4, and it is this:

I want to tell you today about the Director's efforts to preserve and enhance the practice of cryptanalysis in NSA. He has given his personal attention to doing so and has involved top level managers also.

[Redacted]

The thrusts played a prominent part in a Future Sigint Capabilities Study and have been used as bases for planning and budgeting.

Shortly after he became our Director and got his feet on the ground, General Odom enunciated a number of goals for the Agency. He called them "Thrusts" to emphasize that they were to involve present action, not just remote hopes. Briefly stated, the five SIGINT thrusts are:

Last year General Odom held a series of status reviews of all of them, including two review sessions for Thrust #4. One session focused on computers and one focused on personnel. Specific questions posed beforehand by the Director set the stage for these reviews.

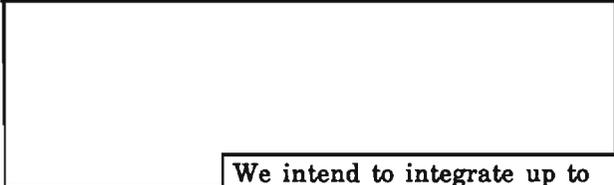
[Redacted]

The first review session, held on 8 Oct 86, concerned computer support for cryptanalysis. It was attended by DIR, DDIR, Chief of Staff, several Key Component Chiefs including DDO, Chiefs of A, B, and G Groups, and the Chiefs of A5, B6, G4, and P1. The Director had asked:

~~CONFIDENTIAL~~

**Update on the Supercomputer Research Center:
Any Actions Dir Should Take?**

ADDR Marlin Wagner discussed NSA's unique needs and applications for massive parallel processing and described SRC progress to date.

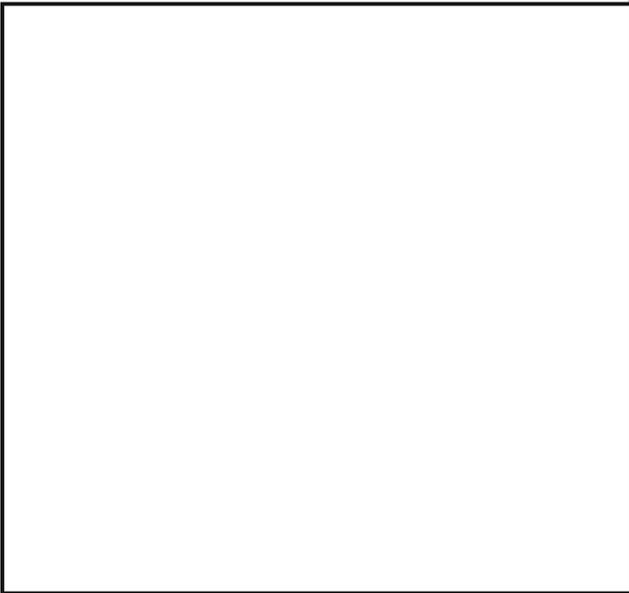


We intend to integrate up to ten NSA professionals in the SRC staff. When it achieves full staffing and operational capabilities in 1988, the SRC will be the



After some discussion, the Director stated his intention to visit the SRC facility and to encourage the Center to intensify both recruitment activities and the assimilation of NSA intees. He also wanted to see a research plan for the SRC.

What is the Significance of Recent and Anticipated Tech Transfers for our Lead in Cryptanalysis?



After considerable discussion of our technical transfer strategy, the Director said we needed to rethink our strategy on high-technology

exports in order to recoup a measure of good will and cooperation with others in the government community, especially the Commerce and State Departments.

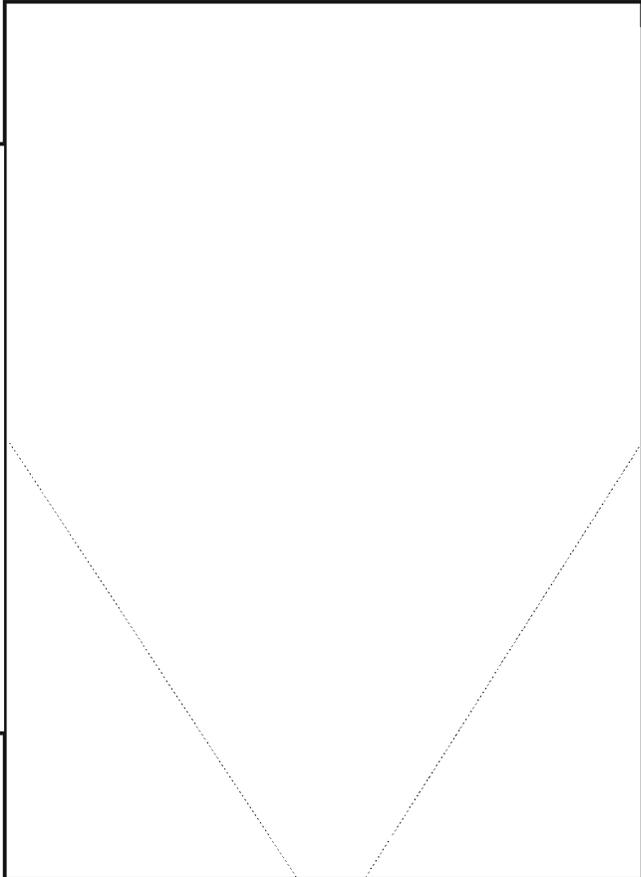
What Should we be Doing about the Semiconductor and Supercomputer Industries?

The concern is that we might become dependent on Japan, for example, for electronic components to use in building computers and special-purpose devices. Chief Scientist K. Speierman had already discussed this question with the Director, so it was not pursued further.

The final question for this session was:

What is the Status of our Computer Acquisition Programs?

How do they fit with Anticipated Parallel Processing Approaches and our Expectations of the SRC?



~~CONFIDENTIAL~~

numbers at all degree levels. However, DDA believed he could meet the hiring goal for mathematicians this year. A discussion followed in which several points were made:

▶ the reason we succeed in hiring PhD mathematicians (who sometimes pass up higher starting salaries elsewhere) is because of the large variety of interesting and difficult problems at NSA;

▶ cryptanalytic mathematicians are becoming more and more necessary in other disciplines such as signals analysis, hardware design, and speech research.

NSA once had an old-boy network of academic mathematicians who had worked in cryptanalysis during the war, who were extremely useful as consultants, and who recommended NSA to their students. This network has mostly disappeared. The Director stated he wanted us to enhance our recruiting methods, aiming particularly at PhD mathematicians (it was agreed that such an effort would also help the recruitment of Masters and Bachelors Degree mathematicians).

What Should We Do to Get More Use from IDA/CRD?

ADDR Marlin Wagner suggested the question should be, "What should we do to get even more use from IDA/CRD?" Those present at the meeting agreed that the contributions from CRD were of high quality and very valuable. The Director expressed satisfaction and there was no further discussion.

The Director's last question was:

What is the Status of Our Last Look at Internal Talent and Inter-Component Relations on Cryptanalysis?

The Chief of P1 (that's me) reported that a group of senior Agency cryptomathematicians from P, R, and S had been organized to

The second review session, held on 9 Oct 86, concerned personnel. It was attended by the same people. The Director's first question was:

Will We Hire Enough New Mathematicians?

DDA Lou Bonanni outlined NSA hiring requirements for mathematicians, the present recruiting program, and some potential problems. One problem is that we are not offering PhD mathematicians a competitive starting salary; another is that American mathematics graduates are declining in

~~CONFIDENTIAL~~~~HANDLE VIA COMINT CHANNELS ONLY~~

~~CONFIDENTIAL~~

consider the need to attract more outstanding mathematicians to NSA, either as employees or as consultants. This group had held one retreat at the Maritime Institute of Technology And Graduate Studies (MITAGS) and had scheduled a second one the same week as this review to plan a Mathematical Sciences Day at NSA for about 50 prominent American mathematicians.

I also said I believed we had an excellent inter-component technical exchange situation involving A5, B6, G4, X1, R51, IDA/CRD,

[redacted] I mentioned the regular seminars (GRABS, the R51 monthly seminar, monthly CMI and KRYPTOS lectures); the Annual Cryptomathematical Exchange (ACE) and annual SCAMP programs; the ad hoc week-long sessions on specific problems; the rotational tours of CA interns, Cryptologic Mathematician Program members, P1 personnel, and others.

Cryptomathematicians at NSA know each other and are able to communicate with each other as needed. (Manual cryptanalysts, however, are in a somewhat different situation, and some changes need to be made; this was not discussed at the review but is being pursued with DDO.) I repeated the earlier view that cryptomathematicians were needed much more widely throughout the Agency than just in cryptanalysis. There was some discussion, and the Director expressed the desire that we determine future skill needs, both qualitative and quantitative, for cryptanalytic work.

Following this meeting, too, the Director assigned a number of tasks addressing issues raised during the review:

▶ He asked DDA (with DDO, DDI, and DDR) to organize a recruiting team of high skill and polish to seek high-quality mathematical talent for the near term.

In response, the MITAGS group worked with M3 to identify Agency mathematicians who should be part of such a team. Also, the Math Sciences Day was held on 6 January 1987; 46 prominent mathematicians attended, some old friends and others new to us. Their expenses were paid and they were housed and fed at the Maritime Institute.

General Odom gave a welcoming talk at NSA in the morning; he said he had two problems he wanted their help with: one problem is how best to operate his proposed program of mathematical research grants [redacted]

[redacted] and the other is how to attract high quality mathematicians to NSA. His talk was followed by some general talks and then some technical ones.

The afternoon program at the Maritime Institute included some unclassified descriptions of math at NSA and how we use mathematicians, and more technical talks, followed by a long session at which we asked the visitors for advice and suggestions about the grants program and about recruiting mathematicians. We believe this meeting was very successful: the visitors gave us many good suggestions; we got some excellent publicity, judging from the feed-back; and we have begun to develop a new boy network that should help us recruit mathematicians in future.

I believe we should hold meetings like this every year.

▶ The Director asked DDA (with DDO, DDI, and DDR input) to propose for his approval a paper defining cryptanalysis in the context of future tasks and of what skills will be needed to do them.

This has been completed.

The definition is quite broad and includes some aspects of signals analysis; some engineering tasks such as the design of special purpose cryptanalytic computers, speech research,

~~CONFIDENTIAL~~
~~HANDLE VIA COMINT CHANNELS ONLY~~

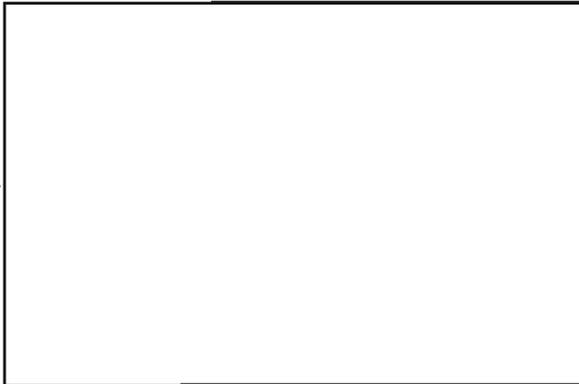
~~CONFIDENTIAL~~

cryptographic system design and evaluation, some aspects of computer security and computer intelligence (a field I believe will emerge in future), and many aspects of computer science, as well as actual cryptanalysis.

▶ He asked DDP (with DDO, DDI, and DDR input) to conduct an "unconstrained" assessment of the numbers of cryptanalytic personnel we will need, and report to him.

The figures emerging from this, all approximate, for actual cryptanalytic work just in Operations are:

P.L. 86-36



▶ He asked DDP (again with DDO, DDI, and DDR input) also to conduct an assessment of the above constrained by reality, and report to him.

▶ Finally, he asked DDA and DDP to take action to ensure that our COSC structure and Table of Distribution accommodate what is developed by the above.

These last three items are still in progress.

It seems clear that General Odom believes in cryptanalysis, is alert to present and future problems, and wants to do something about them. I encourage all of you to take time out occasionally from your daily tasks and give some thought to the future of our unique profession. I invite you to write down any

ideas you may have for improving the practice of cryptanalysis here, for improving the lot of the cryptanalyst, or for any other constructive suggestions, and to send them to me in P1.

Let's help the Director help us! □



Editor's Note: A second review took place in July 1987, just as we were going to press.

BULLETIN BOARD

USERS' GROUP ON SUPERCOMPUTER-UNIX

~~(FOUO)~~ G4 and A5 have established a Working Group to coordinate efforts on supercomputers using UNIX. All organization with users on supercomputers are invited to participate. For more information get in touch with the chairman of the Working Group G45, HQS.

P.L. 86-36

DEVELOPING SOFTWARE?

(U) The second edition of NSA Manual 81-3, *Software Product Standards*, is now in distribution. (For software acquisition the companion document is 81-2.) As DoD-STD-17-3(NS) it is also the DoD standard for use with contractors in software product development and acquisition. A copy can be obtained from T303.

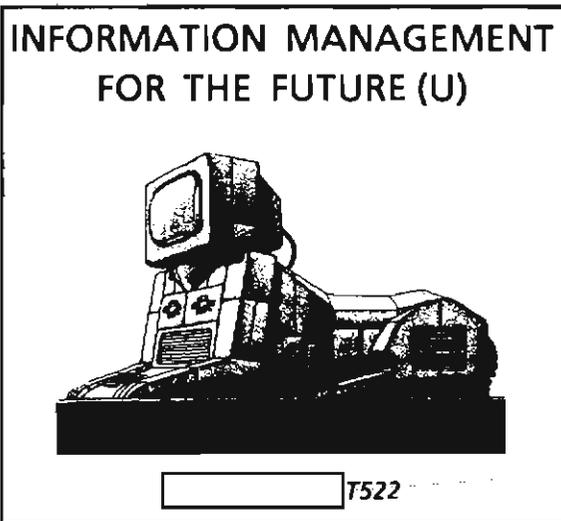
SOFTWARE MANAGEMENT FOR UNICOS

(U) T335 is looking into software management systems for UNICOS. It is willing to investigate and evaluate commercial systems, and also to consider developing an in-house system under UNICOS. Potential users are invited to submit their desiderata (features required or desired) to Jim Bieda, T335.



~~CONFIDENTIAL~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~CONFIDENTIAL~~

(U) John Naisbitt, in his book *Megatrends*, writes, "In the new information society, being without computer skills is like wandering around a collection the size of the Library of Congress with all the books arranged at random with no Dewey Decimal system, no card catalogue--and of course no friendly librarian to serve your information needs." Realizing the import on users, producers, and managers of intelligence information, NSA is taking steps to modernize its traditional information support services to SIGINT operations and to RDT & E efforts.

(U) The information explosion demands a revolutionary approach to keeping abreast of the needs of a knowledge industry. The Agency seniors, as articulated in an December 1983 NSA Advisory Board Report, mandated that a state-of-the-art information support system be developed. The report recommended that the information support system of the future deliver information directly to users via terminal/personal computer systems.

~~(FOUO)~~ The support system will be an integral part of the work life of analysts, managers, engineers, scientists, technologists, and office workers. Supporting these users will be information professionals who will lead in the planning, design, implementation, and maintenance of the system. The success of this endeavor depends on corporate planning, goal-setting, and focused leadership. T5 has been designated as the leader of Agency-wide information resource management. It plans to focus on several key fronts:

- 1) identifying and projecting hardware and software requirements;
- 2) determining proportion of centralized to decentralized support;
- 3) budgeting and control of expenses;
- 4) tasking;
- 5) identifying staffing and skill requirements;
- 6) providing education and training; and
- 7) assessing security requirements and limitations.

P.L. 86-36

~~(FOUO)~~ Further, the advent of the personal computer has added a new dimension to T5's service philosophy "the closer to the customer, the better the service," and has redefined one-on-one service. Computer access will obviate the need for the preferred co-located support, which calls for placing an information professional in an operational element, and instead, enable that professional to provide tailored one-on-one support to several users almost simultaneously.

~~(FOUO)~~ Central to upgrading information support is the Electronic Information Center (EIC). The EIC will facilitate the interaction of all information support functions across organizational boundaries, with T5 as the central management authority. Key entry points for the EIC will be Central Reference, the Scientific and Technical Information Center, the Agency Standard Products Information Center (formerly the Personal Computing Information Center, PCIC), the Agency Records Center, and the Fort Meade Main Library. The EIC will make available major information support and delivery functions that can be accessed by a single log in. It will eventually electronically receive, organize, catalogue, control, process, and deliver all-source information, Agency wide, as needed to support the NSA/CSS missions.

~~(FOUO)~~ The EIC will be a series of personal computers and terminals, linked by a number of local area networks and the Agency Standard Host. The key to the success of the EIC is an easy-to-use, automated method of exchange of information and data among the system components. The programs that compose the EIC are:

~~CONFIDENTIAL~~

~~CONFIDENTIAL~~

P.L. 86-36

► (G) [] Primarily directed toward the support and upgrade of the NSA/CSS libraries and information centers, this program includes the functions provided by [] and a planned acquisition module enhancement. [] capabilities will include an on-line "card" catalog for all library branches, electronic logging of materials, overdue and availability notices, the generation of management and use statistics, material distribution, the status of inter-library loans, procurement documentation, periodical renewals, and mailing labels;

► (G) [] provides direct support in the areas of information research and includes the development of [] (the Time-Sensitive Support Center) [] (commercial database exploitation and delivery), and the Automated Information Support System;

► (U) [] applies to the receipt, storage, and distribution of the majority of incoming electrical and hardcopy messages and material. The primary projects are SOLIS, LEAFLET, WEEDER, DUSTBOX, DOORPLATE, and QUEENSWARE. Each of these programs addresses distinct intelligence collection, dissemination, and management requirements;

► (U) [] modernizes life-cycle records management, with a storage and retrieval system to electronically and automatically archive information.

STATUS OF MODERNIZATION EFFORTS

[] Upgrade of Library

(U) An Electronic Desk has been installed in the Geographic Information Center and was connected to the COINS network to allow on-line research and map display of COINS data. The center is also able to transfer maps to floppy disc for distribution to users.

(FOUO) The Geographic Information Center is now able to produce maps on PCs using the PINSETTER software package developed by P14. PINSETTER enables the analyst to plot and track entities geographically on a PC screen.

(U) LS/2000, the integrated library system, is operational in the NSA/CSS Main Library. It houses cataloging records, which include book and periodical titles, authors, call numbers,

book availability, and information on special collections. A feature of LS/2000 is the use of laser bar code readers.

(U) The ASPIC has expanded its role in production of software for PC and Office Automation (OA) users and will assume a role in the demonstration, acquisition, and distribution of ASH applications software as well. The ASPIC has acquired a Braille printer which enables the Center to produce working aids and tip sheets for the Agency's blind employees.

[] Central and Satellite Modules of the Electronic Information Center

(FOUO) T52 has started to implement [] the automated system designed to transmit, store, and retrieve customer requests for information, references, and documents. The contractor developing and testing [] has begun transferring [] software prototype applications from a PC-base to the 3B20 ASH base. T52 is currently using the PC-based version of INFOREQ applications.

(FOUO) Efforts continue in acquiring and accessing commercial databases for use on ASTWs via dedicated outside telephone lines.

(FOUO) [] a menu-driven gateway which provides access to multiple data bases, is being tested in Central Reference, the STINPO Library, and S2. Databases resident on [] information retrieval systems are already available.

(FOUO) [] an automatic press delivery system, is now operational and available in the Media Center, formerly the Press and Cableroom, 2E099. [] allows automatic delivery of news wire services to the floor of the National SIGINT Operations Center (NSOC). The Intelligence Watch Officer (IWO), a member of the NSOC team, uses [] input to write the IWO Press Review which is distributed to headquarters and field elements.

(FOUO) Conversion of the Press and Cable room has been completed with the delivery of 13 television monitor/recording consoles. Network news and other programs presenting information of concern to Agency analysts are monitored on over 13 channels. The ISO (Intelligence Support Officer) supports the IWO and NSOC desks by monitoring and recording

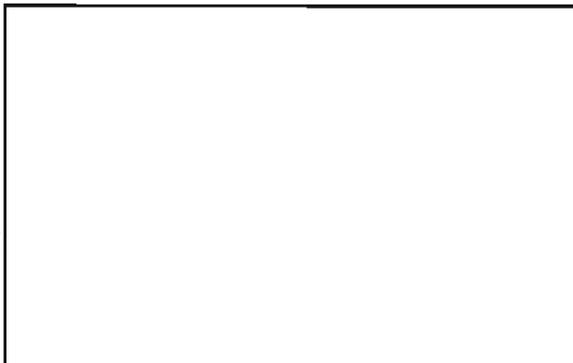
P.L. 86-36

~~CONFIDENTIAL~~

broadcasts and publishing a video news summary. The ISO also makes operationally required video tapes on request.

[redacted] *Modernizing the Handling of Collateral Intelligence Information*

(C) Several SOLIS-like systems have been designed to electronically store, disseminate, and retrieve collateral received by NSA. Those systems available on-line are:



[redacted] *Automation and Upgrade of the Office of Archives and History*

(U) The Office of Archives and History has acquired an IDM 500 database management machine for automated storage and retrieval of archival records.

(U) The Electronic Archiving Division is engaged in a joint effort with the National Archives and Records Administration to study the Optical Digital Image Storage System in order to evaluate the application of optical disk technology to archiving.

⇔

(U) In *Megatrends*, Naisbitt concluded that the most formidable challenge (of the move from an industrial to an information society) will be to train people to work in the information society. The transformation of T5 and its customers into providers and users of an electronic information support network will require a blend of many skills in computer science, intelligence research, information handling and management, personnel management, marketing, communications, and behavioral science.

(U) In order for NSA, a complex knowledge industry, to remain in the mainstream of the information society, the Information

Management Group must meet the challenge to recognize and implement technological and personnel requirements.

FOOD FOR THOUGHT

Extract from

*The Office of the Future:
Information Management for the New Age*

by [redacted] P.L. 86-36

published in *Technology Review*
December/January 1980

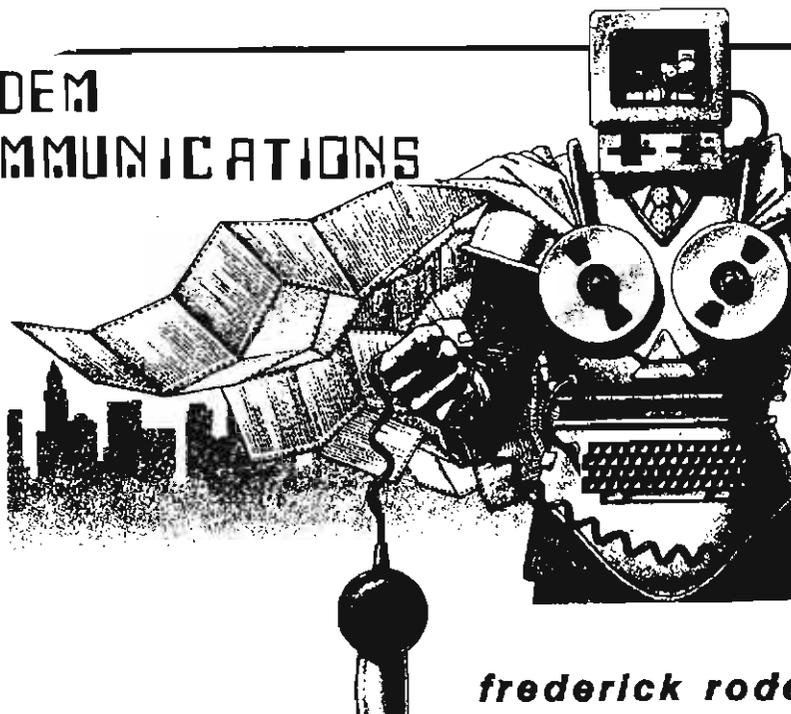
Though there is some variation from organization to organization and from job to job, surveys show that knowledge workers spend the major portion of their time absorbing or giving information verbally. Only a very small percentage of their time is typically given to "thinking" (less than 8 per cent) or to writing (less than 10 percent). The most frequent mode of activity is formal meetings (20 per cent and more in highly structured organizations); two-person conversation on the telephone (5 to 10 per cent) and travel (about 10 per cent) are also important. The proportion of intraorganizational or extraorganizational communication varies over a broad range; knowledge workers in large organizations spend almost all their time talking amongst themselves.

Electronic devices currently available have little direct leverage on the heavy communication loads of knowledge workers. Indeed, the impact of office automation on their personal working habits has been negligible. This is because the communication of knowledge workers is largely unstructured and ill defined. Where memoranda, reports, or procedures are needed, the bulk of the labor is delegated to supporting clerical or specialist staffs; here word processing, text editing, dictation, and facsimile equipment have a definite role. But the idea of automating the illusive, non-standard, and ever-changing communication patterns of knowledge workers remains difficult.

UNCLASSIFIED

~~SECRET~~

MODEM
COMMUNICATIONS
[U]



frederick rodean, g85

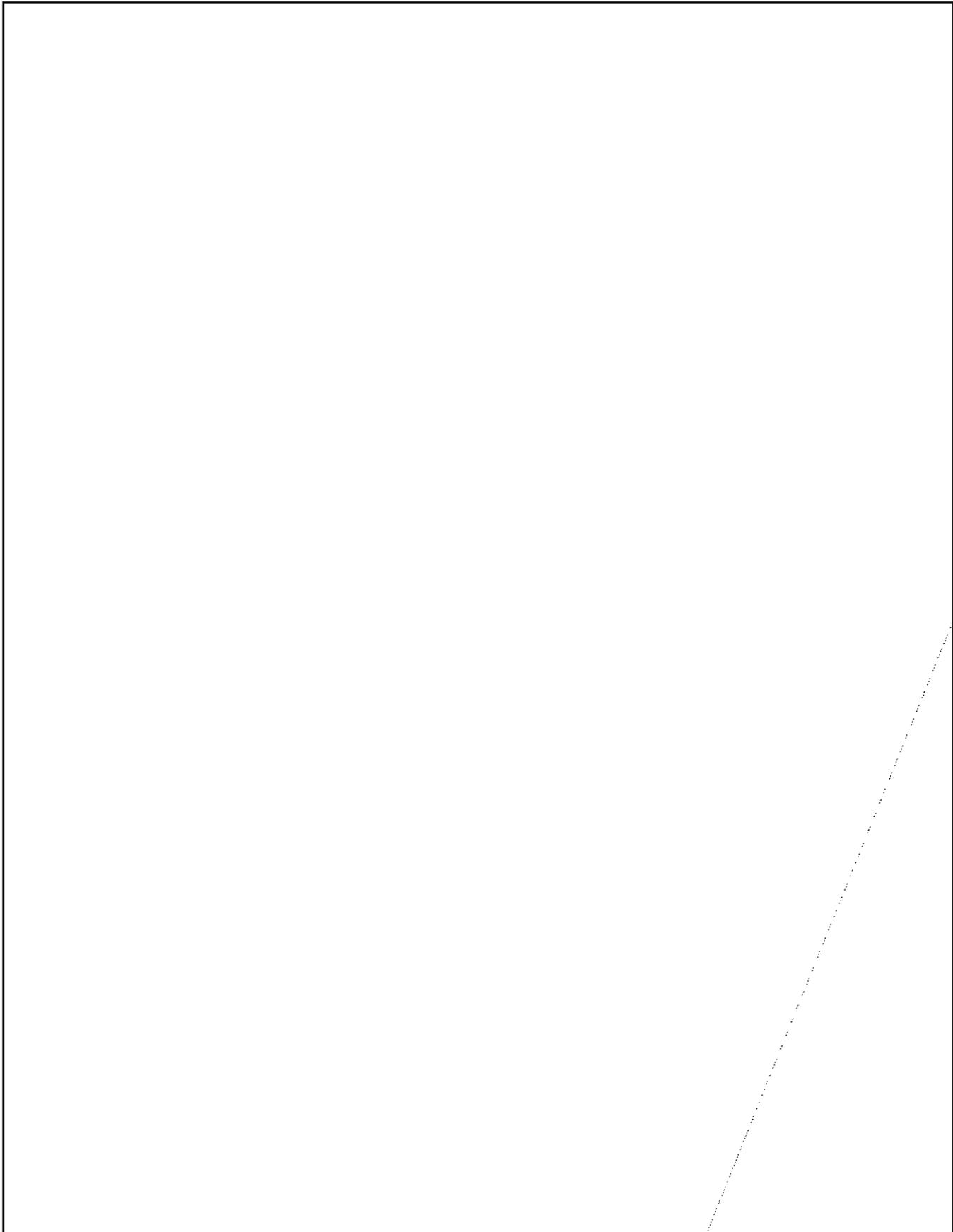
~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~NO CONTRACT~~

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

~~SECRET~~



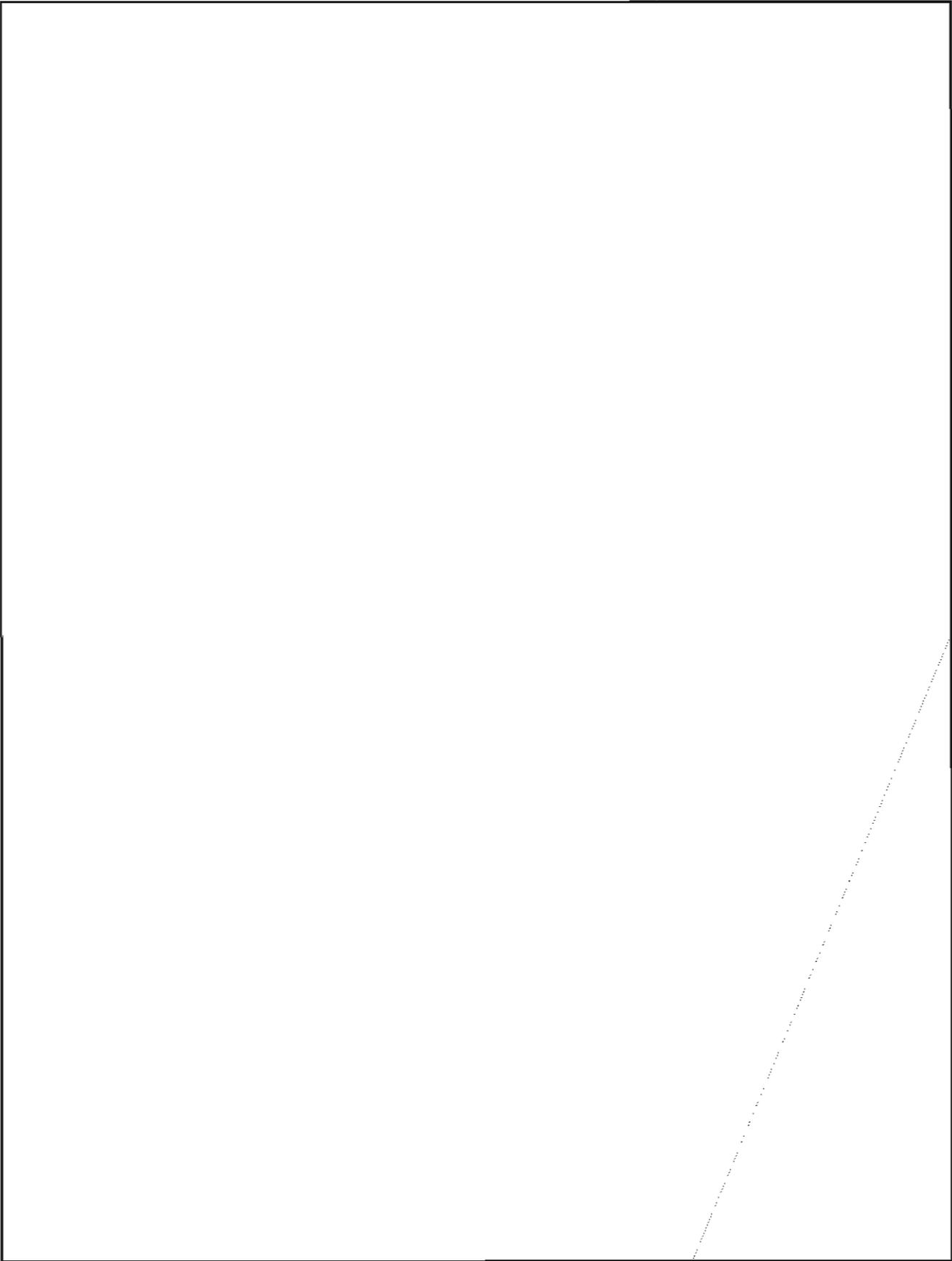
2nd Issue 1987 * CRYPTOLOG * page 10

~~SECRET~~

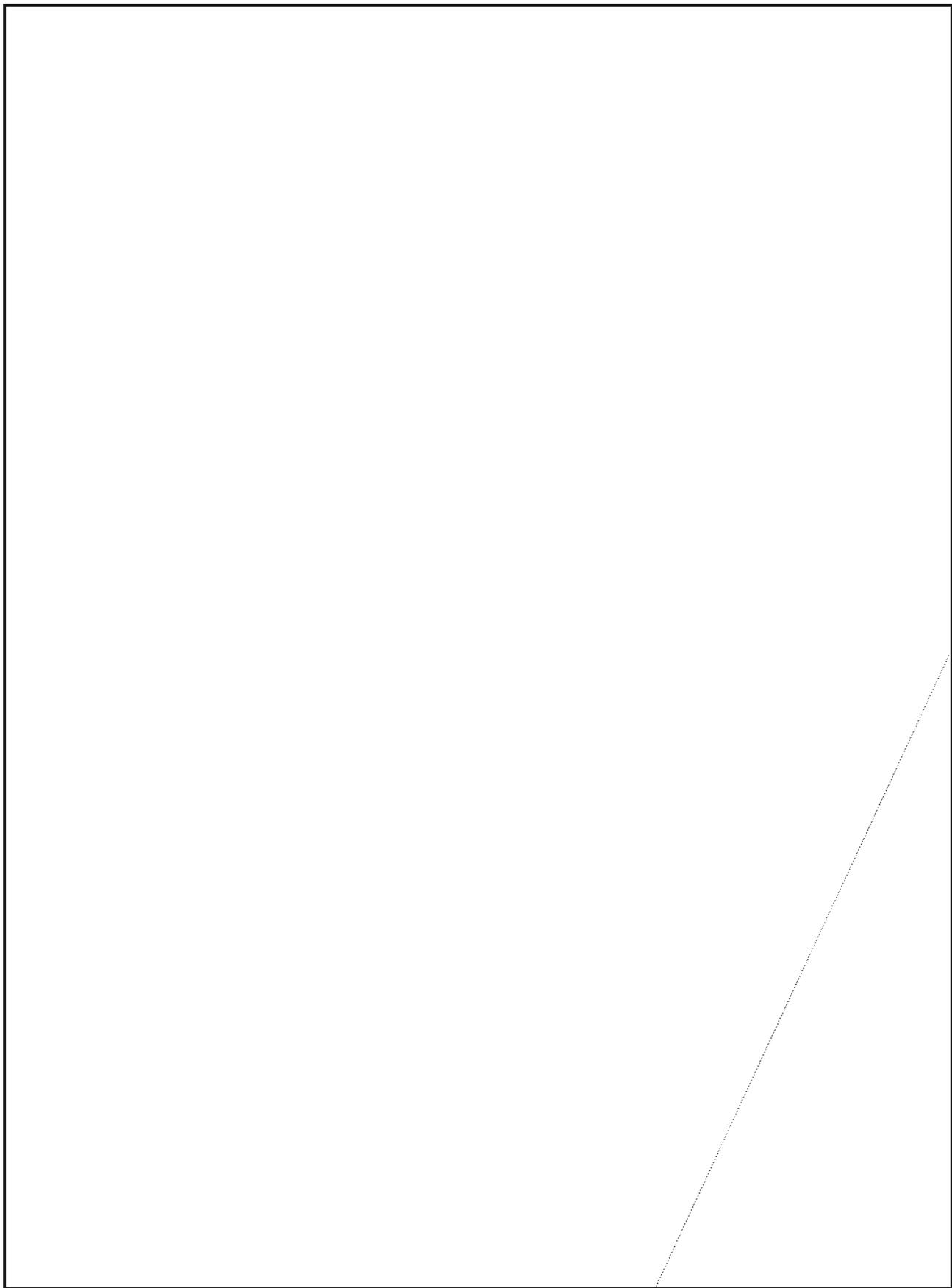
~~HANDLE VIA COMINT CHANNELS ONLY~~

~~NO CONTRACT~~

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



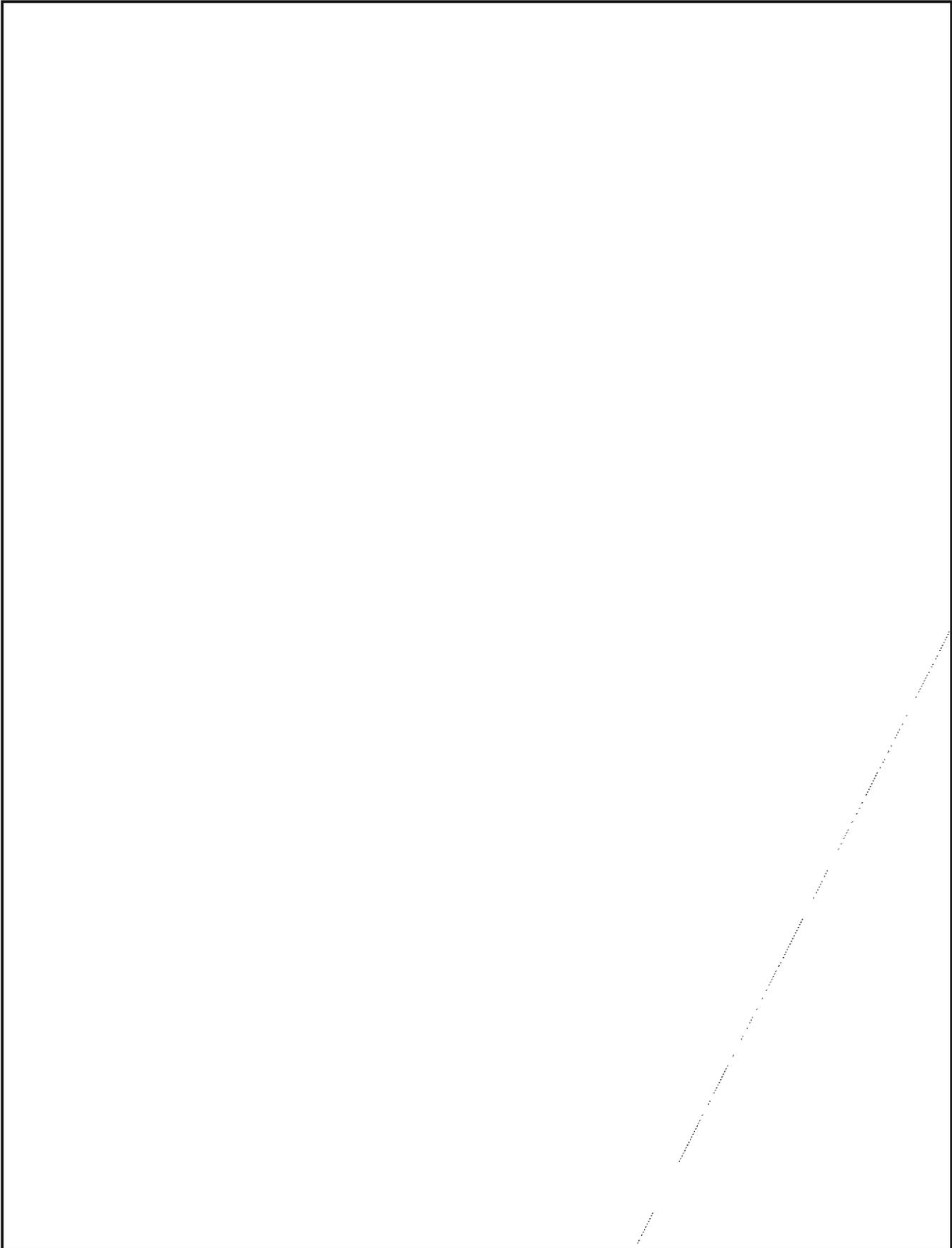
~~SECRET~~



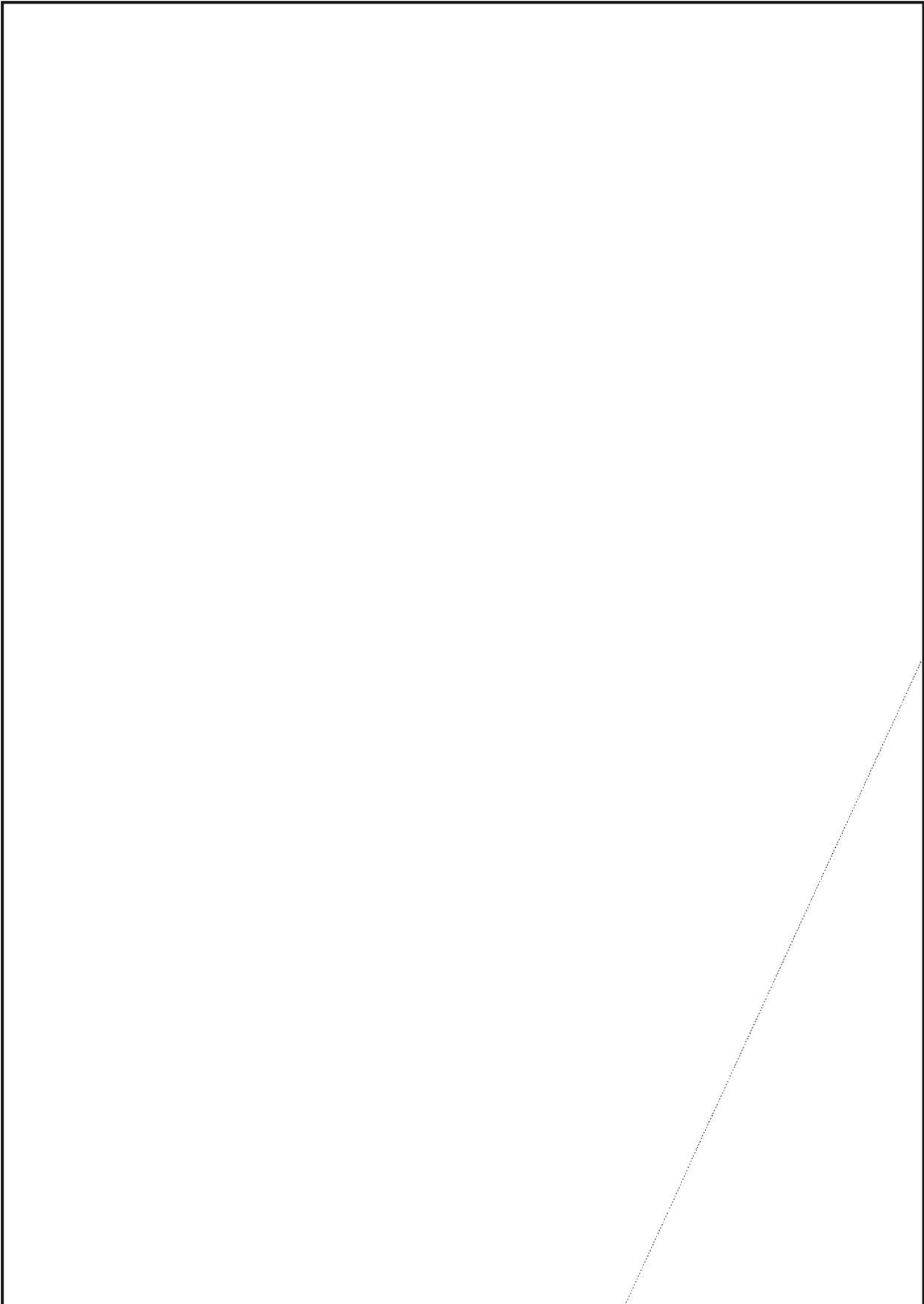
~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~NO CONTRACT~~



~~SECRET~~



2nd Issue 1987 * CRYPTOLOG * page 14

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~

~~NO CONTRACT~~

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

~~SECRET~~

been within the past three years that the performance requirements for satellite networks have begun to take shape.

(U) The basic building block for voice, video and data communication in ISDN is a 64-kilobit per second channel, called a B channel. This same building block is used in existing digital telephony networks to transport pulse-code modulated voice-band signals. To achieve higher transmission rates, several B channels can be concatenated to form a channel with a bandwidth in excess of 64Kbps. The resulting channel is called an H channel.

(U) In existing telephony networks, signaling data for a communications channel is encoded within the channel, while in ISDN, it is carried in a separate, associated channel called a D channel. A single D channel can carry the signaling information for many B channels. This technique of separating the signaling channel from the data transmission channels is called common channel signaling and is fundamental to ISDN.

(U) The trend appears to be towards to the establishment of integrated services digital networks (ISDNs). These networks will carry voice, data, and video information within multiplexed data streams by means of digital microwave, cable, fiber optic, and satellite transmissions. The structure of many of today's packet-switched networks has been designed specifically to facilitate the incorporation of ISDN technology. An ISDN is an end-to-end digital network that uses uniform transmission, signaling, and operating procedures. Access to the network and its associated services will be through a standard, physical interface using existing telephone systems.

(U) The key to ISDN is standards. A committee of telecommunications organizations in Western Europe began work in 1979 to develop standards for ISDNs. Today, ISDN standards are being further defined by the Consultative Committee on International Telephony and Telegraphy (CCITT), an international standards organization with a mandate to establish recommendations for end-to-end performance, interconnection, and maintenance of world networks of telephony, telegraphy and data communications. This group has already identified a number of fundamental standards of ISDN. Interestingly, though, planning for ISDNs has been progressing for at least seven years, it has only

(U) A basic ISDN standard is the basic access interface. This 144-Kbps interface consists of two 64 Kbps B channels for voice, video and data transmission and one (16 Kbps) D channel for signaling. An alternate access interface for large organizations is the primary access interface. For North America and Japan, this is a 1.544-Mbps interface consisting of 23 (64-Kbps) B channels for voice, video, and data transmission and one (64-Kbps) D channel for signaling. In Europe and most of the rest of the world, the interface is a 2.048-Mbps interface consisting of 30 (64-Kbps) B channels for voice, video, and data, and one (64-Kbps) D channel for signaling.

(U) ISDN provides the flexibility of submultiplexing channels for applications that do not require the full 64-Kbps circuit capacity. It also supports packet switching, as well as the circuit switching found in existing networks. These capabilities provide great opportunity to maximize circuit capacity.

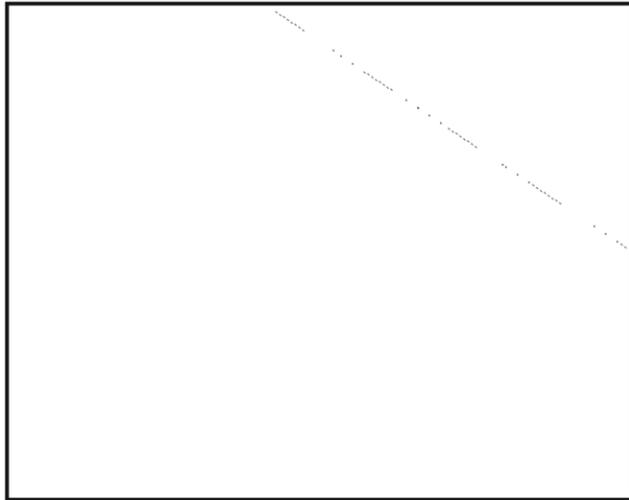
CONCLUSION

2nd Issue 1987 * CRYPTOLOG * page 15

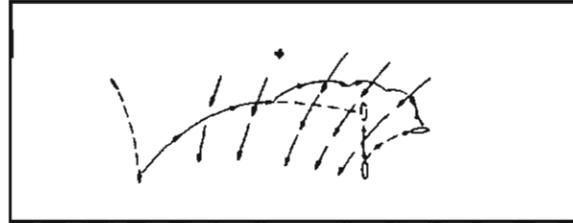
~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~NO CONTRACT~~

~~SECRET~~

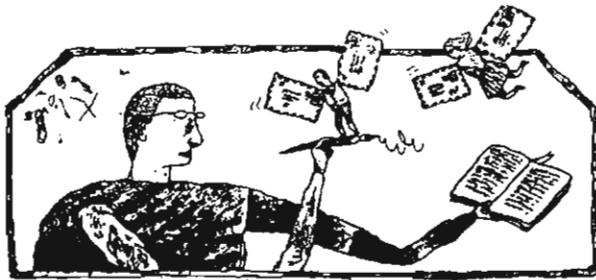


A "piano roll" recording of the frequency hopping sequence.



Mid-course correction to a torpedo course, made by FH-SR-SS communication from an observing aircraft.

LETTERS



To the Editor:

(U) Don't let anyone ever tell you that CRYPTOLOG isn't read. I've had calls from people I don't even know, also from people I hadn't heard from in years ... all because of the Hedy piece!

T542

(U) We, too, have had calls about your intriguing piece, mostly expressing astonishment and delight at discovering that the glamorous Hedy Lamar was co-inventor of a frequency-hopping device.

(U) A couple of knowledgeable readers passed along additional information about the invention, including these illustrations:

(U) Co-inventor George Antheil had composed a multi-player-piano work in the 1920's entitled Ballet Méchanique.

Editor

To the Editor:

(U) On page 10 of the December 1986 issue, you made reference to the United Emirates Republic. A quick check of T5 Working Aid 03-86, "Independent Nations, Dependent Territories, and Their Capitols," dated October 1986, discloses that there is no such national entity. There is however, a *United Arab Emirates*, or the *Arab Republic of Egypt* (formerly, the United Arab Republic).

(U) I hope that not more than 10,000 sharp-eyed editors spotted this error and brought it to your attention.

P.L. 86-36 42405

(U) P.S. The date of this note, when compared to the date of issue of the December 1986 CRYPTOLOG, speaks volumes about the speed of distribution of your estimable publication.

(U) We stand corrected. Thank you. Say, how'd you like to join up as a proofreader?

Editor

(U) P.S. Don't blame Distribution -- we're behind because our @#%+&* terminal has been plagued with hard and soft crashes.

~~SECRET~~

~~HANDLE VIA COMINT CHANNELS ONLY~~
~~NO CONTRACT~~

~~SECRET~~

P.L. 86-36

The Reckoning (u)

 P43

~~(FOUO)~~ Will NSA follow the US automobile industry into becoming a shell organization for offshore producers, sharing its intelligence market the same way Detroit shares its sales market with more aggressive and competent Asian and European suppliers?

(U) In *The Reckoning* David Halberstam gives a long and gloomy account of how the US automobile industry, a self-confident de facto monopoly in the late 1940's, stumbled and blundered into decline, while the Japanese fought their way into the US market and are now well on the way to replacing Detroit as the world center of the automobile industry. There are a number of fascinating parallels between the US automotive monopoly and the US SIGINT monopoly.

(U) Until the 1950's, the Japanese were so awed by Detroit's huge scale of production and technological know-how that they were afraid to go near the US market. They had seen in World War II that US manufacturing technology - in aircraft, ships, vehicles and equipment of every kind - was far superior to anything they could produce.

(U) Halberstam tells the story mainly in terms of the Nissan and Ford automobile companies, which exemplify what happened. The Japanese increased engineering education, and put their ablest people into manufacturing, in every industry they could restart. Henry Ford II, called back from the war to take over the ailing Ford Company, hired MacNamara and his statistical control people to give him

control over the sprawling Ford organization. Over the next twenty-five years the Japanese systematically improved the engineering and manufacture of their cars, while at Ford (and GM) the manufacturing and "car" people steadily lost power to the financial managers who concentrated on keeping up the value of Ford shares to maintain the wealth and social position of Henry Ford II and the Ford family.

(U) The cutbacks and down-grading of manufacturing and of production people in favor of smooth, well dressed "management" people, and the no-risk, quick-profit manipulations led Ford into a complacent production of big, heavy, gadget-loaded cars that gave a high profit per vehicle.

(U) The resistance to new manufacturing investment is illustrated by the incident of the "E-Coating" process, which uses an electrically charged paint bath to get rustproofing paint into every crevice of the body pan. After the process was invented by Ford, GM obtained a license to improve their cars. The Japanese also did E-Coating under licensing. The Ford financial managers, however, rejected the investment cost, and their cars rusted away. It was twenty five years before the Ford production line converted to E-Coating.

(U) In effect, the financial managers became adversaries of the technical people who developed and produced the Ford products. They were profoundly ignorant of car production. For example, to avoid the cost of larger painting bays, MacNamara proposed building the cars in

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

~~SECRET~~

two halves, painting them then welding them together. Henry Ford II had to intervene to block this folly.

(U) The managers grew in power, in spite of their ignorance of cars, by skilled intriguing. The financial managers, directed by Ed Lundy, who took over when MacNamara went to the Pentagon, managed to keep the stock prices high at first by avoiding investments and improvements, but Ford's market share eventually declined as customers bought elsewhere.

(U) Meanwhile, the oil shock of the mid 1970's gave the Japanese expanding access to the US market at the very time that Detroit de-emphasized compact cars. In a telling irony, when Chrysler tightened up its standards for suppliers to match the Japanese quality control and low spoilage, the Midwestern suppliers had to go to Korea to trade off the cheap labor for the new technology investments. This resulted in transferring even more US know-how and manufacturing power to Asian countries, and now they are competing in the US market with the US automobile companies.

(U) Detroit created an adversarial management caste which, by manipulating numbers and quick profit, gave the industry owners and stockholders the impression that they had perfect control of the current operations, when in fact they were losing control of their future to the Asians who paid more attention to technology and production. NSA may well be imitating Detroit by creating an adversarial management caste, with technology and production downgraded, cutback, transferred to contractors, or shipped offshore, in the name of maximizing quick-product and managerial control. Inevitably, there will be a reckoning.

EO 1.4.(c)

P.L. 86-36

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

SOME TIPS ON GETTING PROMOTED (U)
(3rd Edition)

P.L. 86-36
CRYPTOLOG
2nd Issue 1987

Editor's Note: We are very pleased to present this update of an article which has been CRYPTOLOG's all-time best seller. The original, published in the December 1978 issue, was based on a talk given in April 1978 to WIN (Women in NSA); it has been reproduced thousands of times, as has a revised version which appeared in the June-July 1983 issue.

In anticipation of many requests for the 3rd Edition as well, we will have offprints available. For copies send your name, organization, building, room number, and number of copies desired, to: Offprints, CRYPTOLOG, P1, HQS, 8A187. Phone requests will not be honored.

Promotion. The word inevitably stirs response of some kind in every red-blooded NSA employee: hope, pleasure, challenge, despair, frustration, disappointment; even inertia, resentment, resignation. Despite disparate views on promotion, most people share -- openly or secretly -- a common desire to be promoted. And many also share, I believe, a common lack of understanding about the promotion process at NSA and a lack of knowledge about the part they play in it.

This article mainly addresses promotions to grades 13 through 15 and discusses two subjects which are fundamental to those promotions -- Personnel Summaries and Promotion Files. (The Personnel Summaries part also applies to persons in grade 15 for promotion to SCES or STE.) Both are critically important to you, the employee, because they are critically important to the promotion process at NSA. Witness these two points:

- ▶ *your Promotion File represents you to a promotion board, and*
- ▶ *you personally write only one document in that file -- your Personnel Summary.*

Promotion Files described in this article are the ones regularly kept for people in grades 13 and 14, for use by the two NSA-wide Boards that deal with promotions to grades 14 and 15. These Promotion Files are described in the final

section of this article. Promotions to Grade 13 are handled by the Grade 13 Boards in each Key Component; almost all of them also maintain promotion files, with Personnel Summaries, on their Grade 12 employees. Promotions below grade 13 are handled at various local levels and their practices on the maintenance and use of promotion files vary.

Personnel Summaries are important to everyone, regardless of grade. For grades 13 and 14, the formal promotion process requires that every Promotion File, hence every Personnel Summary, be reviewed during every promotion cycle. Personnel Summaries are also used by many of the Key Component Grade 13 Boards, as well as by some of the local boards for grades up through grade 12. (I once chaired a local promotion board in my parent organization, S1, and we routinely reviewed Personnel Summaries of grades 2 through 11 each time we met.)

Personnel Summaries have still other uses: for overseas assignments; for transferring to new jobs; for some types of training. Whenever, in fact, official information on you and your career is needed, the Personnel Summary may be used. The first and major part of this article presents tips on how you should write your all-important Personnel Summary.

The ideas in this article are my own. I was not an expert on personnel matters when I wrote this article in 1978 and did not mean to appear to be. I wrote it as a result of my experience as a member of the NSA Grade 14 Promotion Board that year. In 1980 I chaired the NSA Grade 15 Promotion Board, and later (1981-82) served as a member of the Advisory Panel on Executive Development (APED) which selected candidates for SCEDP. The Executive Development and Qualifications Panel (EDQP) has replaced APED, with expanded responsibilities. The EDQP, a subordinate panel of the Senior Personnel Board (SPB), also evaluates qualifications of potential candidates for the Senior Cryptologic Executive Service (SCES) as well as for service schools and other selections.

These groups all still use employees' promotion files (including the Personnel Summary) during the review process. Files on Grade 15 employees are centrally maintained in M4 and are available for use as needed. All of these experiences have simply confirmed long-held impressions and reinforced my belief about the critical importance of the two topics covered in this article.

PERSONNEL SUMMARIES

Many consider Personnel Summaries to be the bane of their existence. Some don't take them seriously. Others fill them out casually. And most of us write them because we are forced to. Whatever you feel about Personnel Summaries, you should recognize why a Personnel Summary is important, who is responsible for filling it out, when it should be filed, and how to get it filed.

Why Important?

Why is your Personnel Summary important? Because it is an essential document in your Promotion File, the one that describes your complete NSA life: your jobs, your accomplishments, your training, your awards. It is no secret what things are deemed desirable for promotion. The information you provide in your Personnel Summary constitutes a list of the very things judged important when selecting people for promotion, to any grade. Your Promotion File represents you to the Board; it is one of the most important sources of information about you available to them. Board members cannot be expected to have personal knowledge of you in a large Agency like NSA. True, if you are fortunate enough to be nominated for promotion, then a written recommendation about your accomplishments and qualifications is included in your Promotion File. But a new Promotion Nomination form, instituted in August 1986, specifically directs that information available in the Personnel Summary not be duplicated on the Nomination Form. So, **YOUR PERSONNEL SUMMARY IS IT!** Since every Promotion File contains one and you write it, it is your chance to describe what you have done. No one knows it better. And if you do not say it, it may not get said at all.

Who is responsible?

Who is responsible for your Personnel Summary? **YOU ARE!!** You are responsible

for filling it out initially (within 90 days after promotion to grades 12 through 14) and then for updating it. Do not expect your office to remind you. It is your duty. Though Personnel Summaries are not required for them, I also urge people in grades below 12 to fill out Personnel Summaries and to update them periodically. Get into the habit now, for it is easier to do it routinely and gradually than suddenly in one big lump when you become a 12. Also, I think it shows supervisors that you are a person of initiative with serious career intentions.

When to File

As I mentioned in the previous paragraph, you must update your Personnel Summary within 90 days after promotion to grades 12 through 14. I recommend you also do it whenever a major event occurs, such as when you: transfer to a new organization or job; become a supervisor or assume major new duties; receive a major award, professional certification, or educational degree. Otherwise, plan to do it annually, in synchrony with the promotion board cycles. Currently the Key Component Grade 13 Boards meet four times a year; the Agency Grade 14 and 15 Boards meet twice. If your updated Personnel Summary is in your file by 1 February or 1 September, you will satisfy all Boards. (Since both the Promotion Board cycles and members' assignments are now on a fiscal year basis, I recommend September.) I simplify updating my own Summary by following a practice I use to keep track of income tax deductions: whenever anything of importance occurs, I jot it down on a slip of paper with the date and stick the paper into a file. When the time comes to update, I have all the information at hand and the job is nearly done.

Tips on How to Write a Persumm

The following paragraphs describe ways to write a Personnel Summary. These are my personal ideas, and some people -- even you -- may not agree with them. So be it. But I hope to stimulate you to think seriously about Personnel Summaries and to try to help you to write a better one. My aim is to give you a start and hope that you will take it from there.

My best general advice is to be succinct. Say what you have to say briefly, concisely and clearly. Do not write the Great American

Novel and ramble on for 20 pages. On the other hand, avoid being too brief and selling yourself short. (I am surprised at the number of people who write one-liners!) Do not try to upstage Agatha Christie and write a mystery story, but avoid too much excruciating detail. Write your Personnel Summary so that a busy person, who is reading hundreds of Promotion Files, can understand and appreciate it quickly and, you hope, be impressed enough to single

out your file for special consideration. Personnel Summaries are written on form P3267 (REV Sep 78) which is available in the NSA Supply Room, the M35 Integrated Personnel Activities (IPA's) and your office. And now, thanks to office automation, the form is also becoming available as software.

The first page contains seven items. Figure 1 shows the first four:

AS OF (date)		1. NAME (as it appears on official records) (Last, all capital letters)		(first)	(middle)
Feb. 1987		SMITH		JANE	ANNE
2. EMPLOYEE IDENTIFICATION (SSN)	3. CRYPTOLOGIC SERVICE MILITARY (i.e., ASA, AFSS, NSG, NSA) (years) (months)		CIVILIAN (years) (months)		4. TOTAL FEDERAL SERVICE
123-45-6789	3 2		12 9		15yrs 11mos

Figure 1

The "As of" date should never be over a year old. (Some files contain Personnel Summaries so ancient that the paper has turned yellow!) An out-of-date summary raises some rather unflattering -- to you -- questions in the mind of the reader. Are you lazy? Are you so disorganized you cannot remember to update it? Don't you care?

One sees many Personnel Summaries with only the dates changed -- the correction tape over the date is obvious in the reproduced copy. This is often done, and rightly so, to save retyping when there are no major changes to report. But what if there are important changes in your job and you don't record them? Look below at item 6, "Experience" (Fig. 2), taken from a supposedly current Personnel Summary:

6. NSA/CSS OR SCA CIVILIAN EXPERIENCE				
TITLE	GRADE	DATE OF ACTION	AGENCY	ORGANIZATION
A. CURRENT ASSIGNMENT (Functional/Job Title, e.g. Chief, Data Storage Equipment Division; if none, use job title reflected on 3160 or SF 50)				
Traffic Analyst	12	Jan. 1986	.	B111
B. TITLE OF LAST PROMOTION				
Traffic Analyst	12	Apr. 1984		B9
C. INITIAL ASSIGNMENT				
Analyst	5	Jun. 1958		ALLO

Figure 2

To the eye, Item 6 in Fig. 2 looks fine. However, this person is no longer a Traffic Analyst in B111. He has transferred to a new job -- a supervisory one -- and he is now Chief, Processing and Analysis Division, X35. BUT HOW IS THE BOARD TO KNOW?

The problem is magnified if this person is nominated for promotion. The documentation that accompanies the nomination describes the person's CURRENT job, with the result that the two documents -- the nomination and the

Personnel Summary -- do not match. How does that look to a Board? Again, what does it say about you and your sense of responsibility?

When listing your current job title in item 6, be sure to use the FUNCTIONAL job title if you have one. For example: D/Chief, Data Storage Division; Project Manager for XXXX; Russian Language Instructor. Otherwise, use job titles as shown on the form.

Now let's go back to item 5, your educational record (Fig. 3):

5. EDUCATION (List most recent first)			
SCHOOL (Include Joint or Senior Service Colleges; also, any substantial work done toward a degree, but for which no degree was awarded)	DEGREE	MAJOR FIELD	DATES (If great span of time involved, indicate reason, e.g. (Nights))
University of Maryland (Dean's List)	MA (20 credits)	International Relations	1982 - present (Nights)
Armed Forces Staff College	Diploma		1980
University of Maryland (Cum Laude Phi Beta Kappa, Honors in History)	BA	History & Political Science	1972 - 1974
Anne Arundel Community College	AA	History	1970 - 1972
Bowie High School	Diploma	College Preparatory	1969

Figure 3

List these in reverse chronological order, with the most recent first. Include all education for which you earned a degree and use "Diploma" to indicate completion of a joint or service school. Also include substantial work toward another degree. If any of these took extended time, indicate why ("Nights"). And I suggest

you state any graduation honors here, to highlight them.

Item 7, "Commendations and Awards," should also be in reverse chronological order. Fig. 4 shows some examples of the kinds of things to include.

7. COMMENDATIONS AND AWARDS (e.g., Meritorious Civilian Service Awards, Outstanding Performance Appraisals, Letters of Commendation from Chiefs of major organizations or higher) (List most recent first)	DATE
Letter of Appreciation, Chief A	1987
"E" Performance Rating - "our expert on UNIX"	1987
Special cash award (or QSI, or SSWP)	1986
Level 7 Performance Rating	1985
Outstanding Performance Rating	1982, 83, 84
First Prize, CIA Essay Contest	1981
Meritorious Civilian Service Award	1979
NCS Teacher of the Year	1970
NSA Scholarship	1958

Figure 4

Include Letters of Appreciation only if they are from a Chief of a major organization or higher (for grades below 12 I think this rule may be relaxed) and be sure that copies of such letters are in your Promotion File. List only whatever were top-level performance ratings of that period (i.e., when they had them, level-7, but not level-6). I suggest that you add any short complimentary quote from your Performance Appraisal to give it more substance, as "outstanding instructor," "most professional personnelist" or "THE expert." Also list any

special Agency awards (cash or honorary) and scholarships you may have received. Professionalization certifications belong in Item 16, and extra-curricular activities should be entered in Item 14 -- do not include them here.

Page 2 of Form P3267 contains two items. At the top, Item 8 provides space for summarizing your "Current Assignment" (Fig. 5). Begin this paragraph by giving your functional job title, the name of your immediate organization, date of appointment, and names of ascending key organizations.

8. SUMMARY OF CURRENT ASSIGNMENT
D/Chief, Support Staff (Z13), Office of Facilities (Z1), Computer Services Organization (Z)
Since April 1986, Mrs. Jones has been responsible for managing . . .

Figure 5

Then list your major responsibilities, following these recommendations;

- ▶ Use narrative style (not outline form);
- ▶ Use complete sentences;
- ▶ Use third-person forms (not "I was responsible for ..." but "Mrs. Jones was responsible for ...").

Note that your supervisor's signature is required in Item 8 as verification.

Item 9, at the bottom of page 2, is the "Summary of All Previous Civilian and Military Service of a Cryptologic Nature." This is probably the most difficult part of the form to fill out. The longer your career, the more you have to tell about. If there is not enough space provided in Item 9 to hold all the information requested, you should use as many additional plain sheets as necessary, labeling each with your name, SSN, and page number.

This is likely to be the longest section, so it is important to try to make it clear and readable. You do not have to be an accomplished writer or even to have any special writing skill. Just be direct, factual, and as concise as possible. Follow instructions given above for Item 8 (use narrative style, complete sentences, third-person forms).

In addition, follow these suggestions:

- ▶ Use chronological order ("Begin with the oldest assignment and end with the most recent.") Note that this is not "reverse chronological order," as in some of the other items;
- ▶ Use one paragraph per job;
- ▶ Start paragraph with vital information: dates, functional job title, immediate organization and up;
- ▶ Identify organizations, projects, systems, etc.

Notice that I said to identify "organizations, projects, systems, etc." Otherwise, you end up writing a mystery story, like this one:

"From August 1960 to January 1964, Mr. Smith was Chief of A13 where he was responsible for managing all aspects of Project SUCHNSUCH. He also provided technical assistance to several important systems under study by another division: XYZQ and ABCJ."

The only really clear thing in this paragraph is the date! Who remembers what A13 was in the early 1960's? What in heaven's name was SUCHNSUCH? What were systems "XYZQ and ABCJ"? And so on! How much clearer, and how much more professional, if this had been written instead (Fig. 6a):

9. SUMMARY OF ALL PREVIOUS CIVILIAN AND MILITARY SERVICE OF A CRYPTOLOGIC NATURE (List in chronological order begin with oldest assignment and end with most recent; indicate location, functional/job title and dates)

From August 1960 to January 1964, Mr. Smith was Chief of the Nonesuch Reporting Division (A13) in the Office of Overall Reporting (A1) in the General Analysis and Reporting Group (A). He was responsible for managing all aspects of Project SUCHNSUCH (full-text automation of Nonesuch reports) and provided technical assistance to several important systems under study by another division: XYZQ (system for automating . . .) and ABCJ (system for . . .).

Figure 6a

If you wish, you may use a space saving format, with an offset header (for dates, jobs

and organizations) followed by a colon and a list, as in Fig. 6b:

9. SUMMARY OF ALL PREVIOUS CIVILIAN AND MILITARY SERVICE OF A CRYPTOLOGIC NATURE (List in chronological order begin with oldest assignment and end with most recent; indicate location, functional/job title and dates)

August 1960 to January 1964
 Chief, Nonesuch Reporting Division (A13), Office of Overall Reporting (A1),
 General Analysis and Reporting Group (A):

Mr. Smith was responsible for managing: SUCHNSUCH (full-text automation of Nonesuch reports), all reporting on . . ., and providing technical assistance to another division on several important systems, such as XYZQ (system for automating . . .) and ABCJ (system for . . .).

Figure 6b

These may seem like small things to you, but they have a big impact on improving the readability of your Personnel Summary. You do want people to read it, don't you?

As the final test, I recommend that you ask a friend to read your Personnel Summary critically to see if it is indeed clear and to the point. Preferably that friend should pretend that you are not a friend, but a complete stranger who wants to know everything about you. Does your Personnel Summary present you as a clear-writing (and, presumably, clear-thinking), forceful, direct person, or as an imprecise, vague person carrying out "various" unexplained duties? Rewrite your Summary, and especially Item 9, until anyone who reads it -- not just your friends who have known you for years -- can get a clear picture of what you have done and why you are promotable.

Page 3 of the form contains four items, the top three of which are often ignored -- or so it seems when they are so frequently left blank: "Field Assignments," "Related Experience" and "Publications." If you have pertinent information on any of these, put it in.

For Item 10, "Field Assignments" (Fig. 7), be sure to give the organization, functional titles and inclusive dates. These items are in reverse chronological order. Incidentally, regular updating of Personnel Summaries seems to be a special problem for people assigned to the field. Their Personnel Summaries are often neglected while they are away from Fort Meade/FANX and consequently promotion boards sometimes have no knowledge whatsoever about what the person is doing during an important 2- or 3-year period. I urge people to file yearly updated Personnel Summaries while they are on field assignments.

10. CRYPTOLOGIC COMMUNITY FIELD ASSIGNMENTS (CONUS and Overseas) (List most recent first)			
ORGANIZATION	LOCATION	FUNCTIONAL/JOB TITLE	DATES
F06	Timbuck	Chief of Station	1983-86
F99	Eden	Engineer	1970-72
F17	Nowhere	Analyst	1965 (Jan - Mar)

Figure 7

For Item 11, "Other Civilian/Military Experience" (Fig. 8), include those things that

may apply to your NSA job, such as teaching, managing and organizing. These are also in reverse chronological order. For example:

11. OTHER CIVILIAN/MILITARY EXPERIENCE WHICH MAY BE RELATED TO AN NSA/CSS OR SCA POSITION			
ORGANIZATION	LOCATION	FUNCTIONAL/JOB TITLE	DATES
Army Reserve	Ft. Meade, MD	Platoon Leader	1976-Present
G.W. University	Washington, D.C.	Lecturer in Computer Science	1968-70
Summer Camp	Arlington, VA	Director	1965

Figure 8

Item 12 is "Publications" (Fig. 9). I am disappointed that so few files list any publications. Since publications are included in the Personnel Summary, NSA must consider writing to be an important skill. Managers, for example, must spend a lot of time writing. And good writing comes from practice.

Update; Vox Topics. The editors of all these publications welcome your contributions. There are also essay contests sponsored by the Learned Organizations of NSA: CMI, CLA, Kryptos, HRMA, IAI, CISI, etc. And there are opportunities to contribute to the Cryptologic History Series and to NCS courses.

Fortunately for us, NSA offers many opportunities to publish. If you have been looking for places to express your views, here they are: *CRYPTOLOG; The Cryptologic Quarterly; The NSA Newsletter; CLArion, PQS*

Try to have some published works and major reports (though not regular ones produced as part of your job) to list on your Personnel Summary. It just may help to attract attention to your file!

12. PUBLICATIONS (List titles; do not confuse this with reports prepared as a regular part of the job)	DATE
"Project SUCHNSUCH" — A Personal View — article based on talk given in April 1986 to the Computer and Information Sciences Institute (CISI)	CRYPTOLOG Dec. 1986

Figure 9

The next three sections, all part of Item 13 of the form, are meant to show "Highlights in the Area of Self Development" in your professional life -- past, present, and future. The format is the same for all three sections. Fig. 10 gives some examples for "A. Past." List here the things that are completed, such as past

membership in professional societies and education not already listed in Item 5. Courses taken at NSA belong here, but not your college courses. Follow the example and identify the course by title and course number. In the rightmost column, you can indicate things like "Top Student" or special honors. You can leave this column blank if nothing applies.

13. HIGHLIGHTS IN THE AREA OF SELF DEVELOPMENT: (Chronologically list all formal NSA/CSS/SCA, college level or technical courses (military or civilian) as well as membership in either NSA/CSS/SCA or external professional societies) (Exclude those for which a degree was subsequently awarded)

	SUBJECT/SOCIETY	PLACE	DATES (from - to)	DURATION OR LENGTH	DEGREE	SPECIALTY/OFFICE HELD
A. PAST	Zeta Eta Eta (French Honorary)	University	1965-68	--	--	President 1967
	MS-111 (Briefing Skills)	NSA	1968	49hrs	S	--
	MG-444 (Management Analysis)	NSA	1971	120hrs	A	Top Student
	CMI	NSA	1980-Present	--	--	Member

Figure 10

The first two items on page 4, the last page of the form, are "B. Present" and "C. Future" highlights in your self-development (sections not reproduced here). These sections are to be filled out in the same manner as "A. Past." Future plans might include such things as attaining another specified certification, changing your career field or joining a professional society.

Item 14, "Other Achievements" (Fig. 11), provides space for showing your self-development in your nonprofessional life. Many people leave this blank. If you do, I think you are missing a big opportunity to provide a rounded picture of yourself to the Promotion Board. If you are active in the areas like those listed below, I encourage you to list them. Show by your non-job-related activities that you have other interests -- and other talents.

14. OTHER ACHIEVEMENTS (In brief, list all NSA/CSS/SCA affiliate endeavors, which are not necessarily a part of your assigned duties, i.e., Civilian Welfare Council, GEBA, NSA/CSS/SCA club, etc. Civic or Community efforts may be included)

ACTIVITY	INCLUSIVE DATES	CAPACITY IN WHICH SERVING/SERVED
NSA:		
Civilian Welfare Fund	1967 - 1969	B Group representative
Credit Union	1970 - 1973	Member, Board of Governors
GEBA	1972 - Present	Member, Board of Directors
NSA Jazz Band	1979 - Present	Member
Travel Club	1980 - Present	Member, President, 1976-78
United Givers Fund Campaign	1986	Keyman, B Group
Community:		
Church, Scouts, recreational activities, civic groups, PTA	(Provide the appropriate information)	

Figure 11

Item 15 (not reproduced here) provides space for you to list your job-related or self-improvement "Reading Achievements" -- in-house publications, professional journals, foreign language material. Please do not list your pleasure reading,

especially not "Playboy." Board members have seen that one so often they are weary of it! "Professionalization" certifications are to be listed in Item 16 (Fig. 12). If you have more than one, be sure to list them all, with the dates awarded. If you are about to receive still another, note this in parentheses, as shown:

16. PROFESSIONALIZATION (List professional certification(s))

CERTIFICATION		
TITLE	DATE	CERTIFYING PANEL (S)
Cryptanalyst	12 June 1976	Cryptanalysis Career Panel
Education and Training Officer	1 Sept 1983	Education Career Panel
Traffic Analyst (Lack only Part 3 of PQE for certification -- scheduled to take test in Nov 87)		

Figure 12

Finally, sign the form, date it, and affix the proper security classification. Take this responsibility seriously and do it carefully, seeking help from experts if you need it. Underclassifying or overclassifying looks bad to the board because boards expect that by grade 12 you should know how to classify correctly or know where to find help.

Instructions for filling out personnel summaries are contained in the "NSA Personnel Management Manual," Chapter 302B (Oct 79), which every major office has. Your own office will handle the filing of your personnel summary for you. It will reproduce multiple copies of it, some for retention in local organizational files, one for you, and (for grades 13 through 15), some for sending through channels to your promotion file in M4.

PROMOTION FILES

Promotion files are not to be confused with official personnel files, often called "201 Files." The Office of Personnel, specifically the M35 Integrated Personnel Activities maintain them. There is an Official Personnel File for every NSA employee. It documents all formal activity in connection with your NSA life: hiring, performance appraisals, training, job or organization changes, etc. There are official promotion files only for employees in grades 13 and 14. Local organizations often maintain abbreviated versions of the 201 File on their employees and some may also keep a promotion file. Official promotion files are the files that are being discussed here -- the files used by the two Agency-wide promotion boards when considering people for promotion to grades 14 and 15. I am going to tell you what should be in your promotion file, how you can make arrangements to see yours, and how you can update it.

Your Promotion File should contain:

- ▶ *Personnel Summary (current within one year);*
- ▶ *Certification documentation (in the form of a computer printout or a letter from the certifying Panel);*
- ▶ *Recommendation for promotion from Key Component, if you are recommended. (Since Promotion Files are shown to you intact, with nothing removed, you can see the recommendation on you if there is one.)*

In addition, your Promotion File should contain, **FOR YOUR CURRENT GRADE ONLY** (information from previous grades is purged):

- ▶ *Performance Appraisals;*
- ▶ *Inventory of Attributes (If you are 12 or above, this is part of your official Performance Appraisal. However, you may never have seen it or even know it exists because, until the late 70's, it was a private document and was generally not shown to employees. Nowadays the form is white but it used to be yellow and then green, and some files may still contain copies of the older forms.)*

Figure 13 shows the form for the Inventory of Attributes. Rating is on a scale of 00 through 99, and space is provided on the right for narrative comments. Like the information in a Personnel Summary, the items in the Inventory of Attributes constitute a list of some of the most important things (in this case, personal qualities) judged desirable for determining a person's promotability.

You may be concerned about the inevitable unevenness among supervisors' ratings on Performance Appraisals and Inventories of Attributes. Promotion Boards have access to detailed information (large computer runs) about all raters. This information shows them who the "hard" and "easy" raters are and helps the Boards to normalize the ratings.

- ▶ *Cash award and honorary award write-ups;*
- ▶ *Laudatory and commendatory correspondence. (Ordinarily these are to be from Chiefs of*

major organizations or higher. But if you have something noteworthy you would like to include, send a copy to: M43 Promotion Board Room, and let M43 decide.)

- ▶ *Peer group ranking (was used in 1976 only);*
- ▶ *Individual Career Appraisal and Development Plan (used as part of the Performance Appraisal in 1975 only);*
- ▶ *Anything, since your last promotion, that might be beneficial, such as: letters from War Colleges, Invention Awards, Suggestion War Colleges, Invention Awards, Adjunct Faculty certificates from NCS, etc.*

To review your Promotion File, call Mrs. Alice M43, on 963-1677s or 688-7611b and make an appointment to see her, in Room 2B4132. You may talk to her about adding items to your file if you notice that something is missing. And if you disagree with something in your file or think that it is incorrect, call her attention to it. Depending on what it is, she may suggest that you discuss the matter with your supervisor, and then advise you about the possibility of your inserting something in the file to explain your views, as is usually allowed. M4 encourages you to look at your Promotion File and welcomes your help in keeping it up to date and complete. To insure that it is, especially if you have something important to add just at the time the Boards are conducting their file reviews, you should send a special copy directly to M43-Promotion Board Room as well as through official channels.

In conclusion, two points already mentioned sum up the main ideas with which I would leave you.

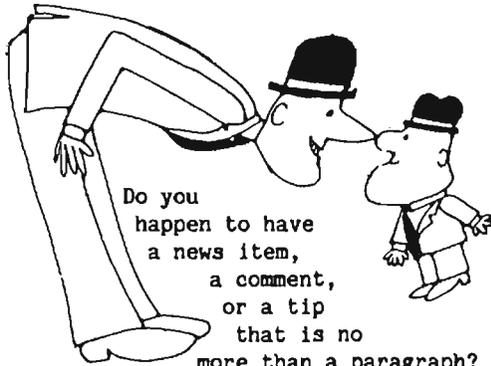
Your Promotion File represents YOU;

YOU write YOUR Personnel Summary.

Improve your promotability! Increase your chances of getting promoted by making sure that your Promotion File is complete and that your Personnel Summary is up to date and clearly written. It's up to you!



Contributions Solicited



Do you happen to have a news item, a comment, or a tip that is no more than a paragraph?

Or perhaps you have an article of several thousands words? Long or short, if it has something worthwhile to say, we'll probably print it. Of course, a shorter item has a much better chance of getting read. (For your interest and guidance, one page of typescript, double-spaced, makes about one column in CRYPTOLOG.)



Your contribution does not have to be typed; we'll give preference to content over form, every time. (We've even accepted an item written on a used lunch bag!) Nowadays most people use a word processor, and in

that case we ask you to send a floppy along with the hard copy, and write on your floppy what hardware, operating system, and word processing software you used. (And don't forget to include the file name and your name and phone number.) You can also send items via electronic mail to cryptlg@bar1c05. In either case, please do not right-justify in your soft copy; the spacing isn't the same in our columnar format, and the extra spaces may have to be removed by hand, one by one -- in this day and age of automation!

First-person articles or stories about your own experiences are welcome, so long as they relate in some way to our work.



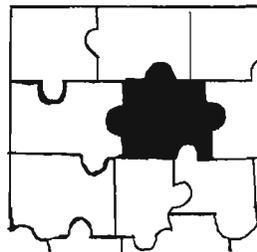
Want anonymity? A thoughtful piece on a subject of interest to a large number of readers will be considered for anonymous publication if the writer requests it. The writer must, however, identify himself or herself to the editor. Needless to say, personal or trivial complaints will not be considered.

Need assistance? You may have an idea, or some notes, or even a half-finished paper that you feel has possibilities but you don't know what to do with. A call to the appropriate subject editor will get you a "story conference" and possibly inspire you to finish it up and get it into print.



Sensitive materials? No way!!! We'll go all the way to Top Secret Codeword, but we have to draw the line at compartmented or otherwise sensitive information.

Something missing? If you feel that your work or your interests are not represented in CRYPTOLOG, it's probably because you and your friends are not contributing. The editors earnestly want to cover the whole territory, but articles don't grow on trees, y'know! Somebody (who knows the subject matter) has to write them.



Our deadline? Theoretically, we should have one, but we don't. After all, CRYPTOLOG comes out six times a year, so if we get your article just after one issue has gone to press, you'll be in time for another one. There's no such thing as a bad time to submit an item for publication in CRYPTOLOG.

S	M	T	W	T	F	S
						4
5	6	7	8	9	10	11
12	13	14	15	16	17	18
19	20	21	22	23	24	25
26	27	28	29	30	31	

GETTING STARTED

1. My object is to:

- Make a report on something that has been accomplished
- Call attention to something that is wrong
- Suggest a better method or idea
- Share a personal experience
- Enlist support
- Explain a process
- Ask a question
- Defend a principle
- Report news or announce a coming event
- Recognize an achievement
- Amuse and entertain
- React to something someone else has written
- None of the above, but something else, namely: _____

2. My working title is:

- A better way to _____
- Hurray for _____
- The fallacy of _____
- It's time to _____
- The scandal of _____
- Are we paying too much for _____?
- After _____, What?
- A proposal for _____
- What happened at _____
- Why I agree/disagree with _____ who wrote _____
- A funny thing happened on the way to _____
- None of the above, but _____

3. I will consider this, in my own mind, an open letter to _____ and will address to primarily to her/him/them.

- 4. This would be a particularly good time for such an article to appear because _____ (or)
- This subject is timeless

- 5. I am especially well qualified to write on this because _____ (or, on the other hand)
- I want to speak up on this even though I am no expert on it, because _____

6. Some tentative suggestions for a final title are: _____

7. I think it would be most appropriate for publication in:

- CRYPTOLOG
- The Cryptologic Quarterly
- CLARion
- The NSA Newsletter
- PQS Update
- Vox Topics

Golden Oldie (U)

EMPLOYEE PERFORMANCE APPRAISAL PART A			<input checked="" type="checkbox"/> OFFICIAL <input type="checkbox"/> UNOFFICIAL
LAST NAME - FIRST NAME - MIDDLE INITIAL CLICHE, Paragonia A.		TITLE, GRADE AND JOB NUMBER Cryptanalyst (F/L), GS-9 NSA-6829	
INSTALLATION NSA	ORGANIZATIONAL SEGMENT 7122	APPRAISAL PERIOD FROM 29 Feb 55 TO 29 Feb 56	
<p>1. SUPERVISOR'S EVALUATION OF PERFORMANCE ON THE ABOVE JOB: <i>(Covers aspects of performance as outlined in Performance Appraisal, a reference manual for supervisors)</i></p> <p style="text-align: center;"> She's as potent as nuclear fission In advancing the Agency's mission Her cooperation approaches perfection She GETS ALONG WELL WITH OTHERS IN SECTION Paragonia's got a surplus Of SERIOUSNESS OF PURPOSE And nobody downgrades this cutie When it comes to DEVOTION TO DUTY. She's got TECHNICAL ABILITY EMOTIONAL STABILITY And QUANTITY and QUALITY And USEFUL VERSATILITY. She can COORDINATE and EXPEDITE INITIATE - and read and write And on the POST She's the MOST In ATTENTION TO PERTINENT DETAIL She exercises JUDGMENT (ROUND) As well as LEADERSHIP (ALL ROUND) To no avail. For though she's all these gorgeous things This paragon of skill on wings Gets! Performance Rating: SATISFACTORY </p> <p>MAJOR STRENGTHS:</p> <p>MAJOR AREAS IN WHICH IMPROVEMENT IS DESIRED:</p>			
2. PERFORMANCE RATING: <input type="checkbox"/> OUTSTANDING <input checked="" type="checkbox"/> SATISFACTORY <input type="checkbox"/> UNSATISFACTORY <i>(Justification attached)</i>			
EMPLOYEE'S SIGNATURE		DATE OF DISCUSSION	SUPERVISOR'S SIGNATURE AND TITLE
<p><i>NOTE: The adjective rating assigned may be appealed. Information on the appeal procedure may be obtained from your supervisor, or if you prefer, from the Civilian Personnel Office.</i></p>			

DA FORM 1052 (TEST)

NSA-CROSTIC # 64

R822

*The quotation on the next page was taken from a published work of an NSAer.
The first letters of the WORDS spell out the author's name and the title of the work.*

DEFINITIONS

WORDS

A. Operate unobstructedly	80	152	140	119	7	167	85	29	36
B. Freshness	63	173	3	188	104	117	57		
C. Blameless	8	122	47	191	58	12	171	114	
D. Reflected	196	65	102	111	133	71			
E. Miss Marple does it	68	49	148	34	110	62			
F. ----- love	195	176	66	10	16	160	186	75	
G. Bow partners	170	44	150	2	106	88			
H. Having a certain visual defect	154	138	14	146	202	37	157	84	166
I. Once famous for its trees	108	39	51	161	1	46	26		95
J. Boredom	201	86	94	22	156				133
K. Fanny Farmer measure	135	116	180	165	87	10			
L. George Washington had one	163	181	31	88	151	25	48		
M. Steadfast	64	112	15	93	178	109	27	158	172
N. Input again	185	81	118	133	144	77			
O. Provided gratuitously	130	162	192	53	17	126	90		
P. ----- measure	198	24	121	183	38	136	97		
Q. Pronoun	70	127	184	197	145	139	177		
R. Information source	60	98	81	45	142	19	199	189	5
S. Economic doctrine	190	79	73	107	174	51	8	18	113
T. ----- baron	81	59	91	132	168	119			179
U. Wished	92	6	74	137	40	193	169		
V. Rear deck	42	4	21	52					
W. Seat for an amphibian	100	162	76	120	175	33	143	159	56
X. Advancing	54	32	124	147	99	194	61		
Y. Long-term rental	35	123	105	129	89	125	153	50	30
Z. Commencement	164	128	23	78	67	41			
a. Transmission	200	72	103	55	76	149	96		
b. Barms	187	43	134	13	101	141			

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

HOW RUSSIANS VIEW THEIR LEADERS

A story is making the rounds in the Soviet Union and in some Eastern Bloc countries describing how the Party Chairmen would have dealt with a problem:

A train is traveling from Moscow to Siberia when suddenly the rails end. What to do? Await orders from Moscow, from the Kremlin.

Under Stalin, the order is given:

"Everyone off the train. Shoot everyone."

Under Krushchev:

"Everyone off the train. Pick up the rails from behind the train and lay them ahead. Move forward. Pick up the rails from behind the train and lay them ahead." And so on ...

Under Brezhnev:

"Everyone stay on the train. Close the blinds and rock the train so that everyone will think it's still moving."

Under Gorbachev:

"Everyone off the train. All loudly shout, "There are no rails!!! There are no rails!!! There are no rails!!!"

Provided by: P16

Answers to:

"NSA" PUZZLE

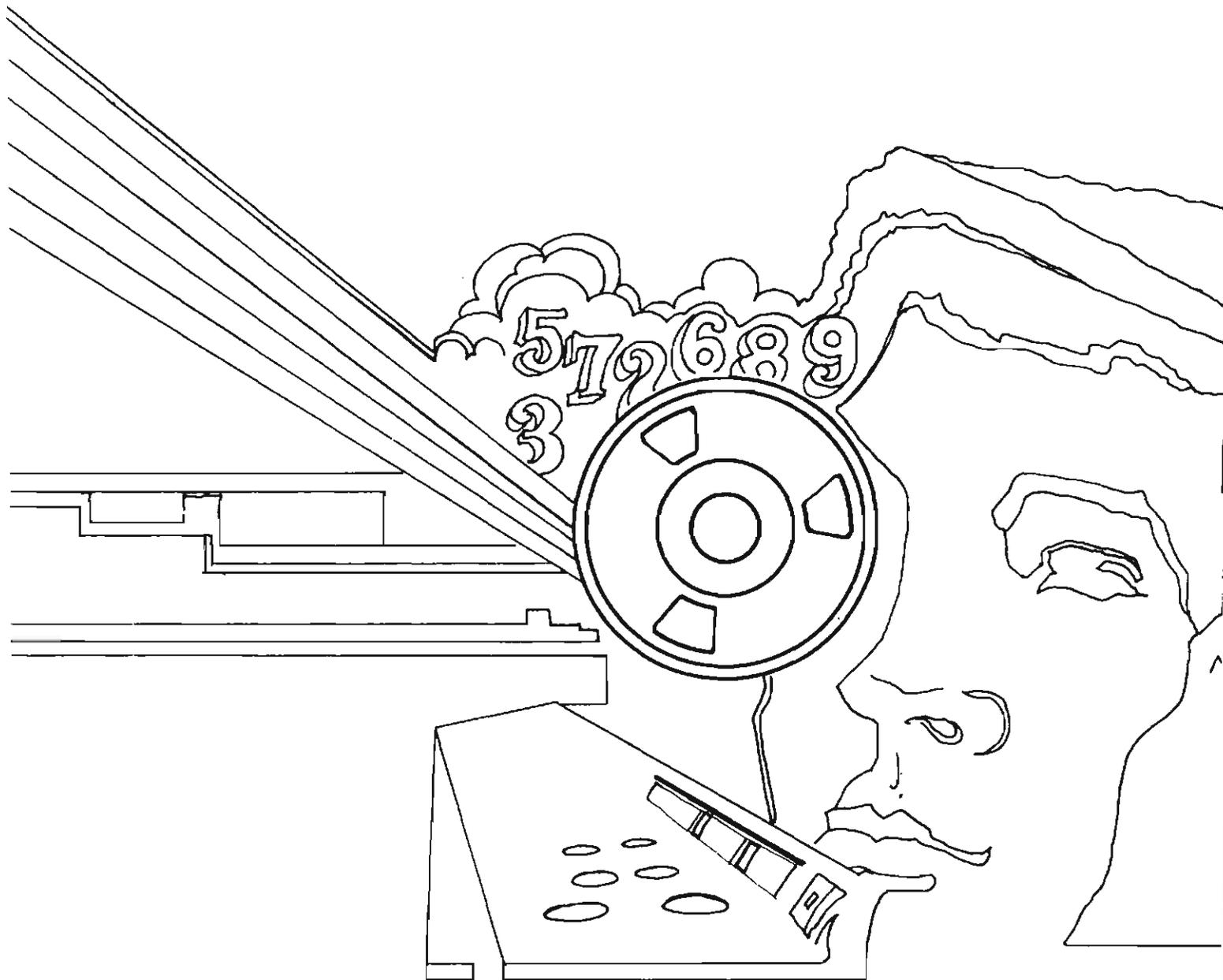
(1st Issue 1987)

by Carolyn Cornelius, T12

1. INSANE
2. ARKANSAS
3. UNSALTED
4. COMPENSATE
5. BONSAI
6. INSATIABLE
7. TRANSATLANTIC
8. CARAVANSARY
9. INSALUBRIOUS
10. UNSAID
11. RANSACK
12. GAINSAY
13. UNSALARIED
14. CONSANGUINITY
15. UNSANITARY
16. TRANSACTION
17. UNSAVORY
18. MANSARD
19. MAINSAIL
20. UNSATURATED



~~SECRET~~



~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~