

~~SECRET~~

NATIONAL SECURITY AGENCY  
FORT GEORGE G. MEADE, MARYLAND

# CRYPTOLOG

MAY 1985



P.L. 86-36

THE G4 PLAN FOR CAREER DEVELOPMENT (U).....		1
THE CRYPTOLOGIC LINGUIST PROGRAM (U).....		4
THE SUMMER LANGUAGE PROGRAM (U).....		4
COPING WITH CAREER CHANGE (U).....		5
CA SKILLS ENHANCEMENT PROGRAM (U).....		6
GALAXY (U).....		7
THE FUTURE OF TRAFFIC ANALYSIS (U).....		9
LETTER TO THE EDITOR (U).....	Robert J. Hanyok.....	10
FROM THE PAST (U).....		11
CRYPTO-PUZZLE NO. 29 (U).....	William Lutwiniak.....	12
NSA INTERN TRAINING PROGRAM [1955] (U).....		13

~~HANDLE VIA COMINT CHANNELS ONLY~~~~SECRET~~~~CLASSIFIED BY NSA/CSSM 123-2~~~~DECLASSIFY ON: Originating~~

# CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XII, No. 5 ..... May 1985

PUBLISHER ..... [redacted]

## BOARD OF EDITORS

Editor ..... [redacted] (963-1103)

Collection ..... [redacted] (963-5877)

Computer Security ..... [redacted] (968-8141)

Computer Systems ..... [redacted] (963-1103)

Cryptanalysis ..... [redacted] (963-4740)

Cryptolinguistics ..... [redacted] (963-4704)

Index ..... [redacted] (963-5330)

Information Science ..... [redacted] (963-5711)

Intelligence Research ..... [redacted] (963-3095)

Language ..... [redacted] (963-5151)

Linguistics ..... [redacted] (963-3896)

Mathematics ..... [redacted] (963-5655)

Puzzles ..... David H. Williams (963-1103)

Science and Technology ..... [redacted] (963-4423)

Special Research ..... Vera R. Filby (968-8014)

Traffic Analysis ..... Robert J. Hanyok (963-3888)

Illustrator ..... [redacted] (963-3057)

Distribution ..... [redacted] (963-3369)

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

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 equip-  
ment and what software you used.

via PLATFORM mail, send to:  
cryptolg at bar1c05  
(bar-one-c-zero-five)  
(note: no 'o' in 'log')

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

For Subscriptions or Change of Address  
send name and organization to:  
[redacted] P14

P.L. 86-36

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

## Editorial

P.L. 86-36

In this issue we commemorate the 20th anniversary of the Career Development Program. It was celebrated in the Agency by a week-long series of presentations, discussions, and seminars. Two of these are reported in these pages; others will appear in subsequent issues.

The professionalization program certainly has taken hold. Now there is a certification procedure for just about every calling in NSA: for executive secretary as well as for cryptanalyst; in logistics as well as in language. Over the years there have been modifications, too, reflecting changes in philosophical outlook, changes in our targets, and advances in technology. (It would be fun to check out the "pqc" of 14th century Venice.) New fields have been recognized and added, and two -- cryptologic staff officer and editor-writer -- have been dropped. And one field -- intelligence research is its latest appellation -- has always been in the throes of change.

What is significant is that most operational elements are seeing to it that their direct-hire pre-professionals are given the training and work assignments necessary for certification, though perhaps at a slower pace than that set for interns in the same fields. One element has even developed for its own people a very successful formal program patterned after the CA program.

Some people wonder not at the longevity of the program, but that it is only 20 years old. Why did it take so long, to get going, they ask. Actually, there were earlier attempts at a development program: the intern training program of 1955, the PATA program and CY-100 (even CA-400 in its infancy) come to mind. But they were very different in concept; the participants consisted of a small segment of the population who were to be the future leaders, having first undergone a rigorous course of formal instruction or OJT with a focus on cryptanalysis. It would be interesting to hear from participants in those or other similar programs and from people who had a hand in designing them.

~~FOR OFFICIAL USE ONLY~~

~~CONFIDENTIAL~~

## The G4 Plan for Career Development



(U)  
42

P.L. 86-36

~~(FOUO)~~ For many years, vacant billets in G4 for professional or pre-professional jobs at the middle level were usually filled with graduates of intern programs, notably the P1 Math Program and the Cryptanalysis Panel, and from other panels as well. By 1981, however, G4 was beginning to increase the number of new billets and soon exceeded the capacities of existing training programs. A few college graduates were hired directly into G4 where they received on-the-job training (OJT) and were enrolled in certain relevant courses offered by the training school. To fulfill its ever-expanding mission, G4 made further plans to increase sharply the number of direct college hires for the next several years.

~~(FOUO)~~ In order to attract the best candidates, the chief of G4 [redacted] thought it wise to afford them the same opportunity to attain professional certification, usually in cryptanalysis (CA), in three years' time as those entering a formal intern program. As Chairman of the Cryptanalysis Career Panel he was well versed in the requirements and the ways to satisfy them. He devised a plan that would lead to professional certification and at the same time prepare new hires for their careers in G4 -- the specialties of their home branch where they are assigned, on the one hand, and a view and appreciation of the varied and complex mission of all three divisions within G4 on the other -- in production as well as in analysis, research, and developing new techniques.

### IMPLEMENTATION

~~(FOUO)~~ By August 1982, Jim had formulated his ideas and asked the author of this article to be coordinator of the plan. He outlined to me, as well as to the three division chiefs, the diversification tours he had in mind to satisfy the two goals of CA certification and preparation for careers in G4. He quickly and easily convinced me of the worth of this career development project; I not only believed in it, I knew it was good. As coordinator I saw my role to be a combination of "travel agent" -- arranging diversification tours -- and "faculty adviser" -- informing the new college hires of the requirements, recommending relevant courses, and

encouraging them in these worthy endeavors for their own future and upward mobility.

~~(FOUO)~~ To this end, I devised various ways to keep track of their progress toward the goals, such as charts and worksheets for planning tours. As the number of new college hires has grown, we have turned to the IBM PC, recently made available, for help in this regard.

~~(FOUO)~~ The Plan has its own floppy disk. [redacted] of G424 designed a comprehensive, yet easy-to-use package to retain pertinent and useful information that can be easily updated. This will be a boon when an avalanche of new college hires engulfs us later this year.

~~(FOUO)~~ [redacted] G409, is invaluable in the preliminary billet preparation, initial counseling of the new hires before assignment, and seeing to the formal personnel actions. [redacted] G409, carries the ball on training requests for specific courses. Most of all, the help, advice, and cooperation we received the first year from the then CA Panel executive [redacted] and his assistant, [redacted] enabled us to get off the ground quickly and attain the momentum for our fast track.

~~(FOUO)~~ Fortunately, for all of us -- me, the new college hires, and their branch chiefs -- the selection process provided us with a group of winners. Most of them were able to get on the fast track and, with a push from me, traveled to other realms for diversification and experience, digested relevant courses, and thrived on OJT. Those who had had algebra, statistics, and/or computer science in college satisfied most of the prerequisites for relevant or advanced courses, which they could sign up for without delay. They plunged immediately into learning to program in IMP; some floundered a bit longer than others, but all have survived and have become able and talented programmers.

~~(FOUO)~~ As for the tours, in less than a month (by early September 1982) we were off and running. Among the group of newcomers who had joined the Agency and G4 the year before, 1981, there were five who had had at least six months' experience. They were our first pioneers for the new set of diversification tours.

~~CONFIDENTIAL~~

## STATISTICS ON THE G4 DEVELOPMENT PLAN (U)

EOD G4		P.L. 86-36 EO 1.4. (c)	SAT FOR EXAM	PASSED
1981	5			
1982	15			
1983	14	Part I.....CA	19	19
1984	7	Part II....Related Fields	19	19
1985	11	Part III...Essay	19	18
Total	52			

## TOURS

~~(C-CCO)~~ Happily, the two goals of the G4 Plan can be met with a set of designated tours of six months or more each:

1. G41 - for production experience
2. G42 - for diagnosis and techniques
3. G434 - [ ] and production
4. Manual Systems - for CA diversification
5. An optional tour at the discretion of each division

When new college hires have finished the indoctrination course (CY-157) at Airport Square and received their clearances, their initial assignment to a branch in G4 (hereafter referred to as their "home" branch) constitutes one of the first three tours specified above. After six months or longer, they are considered ready for a tour in another area. Upon completion of some or all of CA-107 they are eligible for a tour in manual systems.

~~(C)~~ We soon found that training slots were in great demand. The CA Panel had hired that same year, 1982, a bumper crop of interns that filled the usual spaces in G6 and G9. In desperation we hunted elsewhere and found tours eventually in A3, B1, B5, G2, and P16 for manual systems. When all the available training slots for manual systems were filled, we scheduled other tours in G4 for our group. We were only too happy to cooperate with the CA Panel and made a point of yielding to them on these matters.

~~(FOUO)~~ We also explored other parts of the Agency for the optional tour. At first, G42 specified another tour in a different type of branch within G42; but we have by now extended the range to include S6, and will soon include A5 as well. As for G43, a tour in G431 is appropriate, and tours in W3, R5, and R8 have also been scheduled. In this way a branch can acquire expertise from different areas as the new college hires complete the optional tours and return "home" to stay.

~~(FOUO)~~ Another way to arrange tours is to agree to an exchange, i.e., providing a tour in G4 to someone assigned elsewhere who needs a diversification tour also. We have had to make these double arrangements four or five times in order to keep to the fast track schedule. One or two branch

chiefs want their new people to do all their tours back-to-back before returning "home;" their projects are usually long-term and not easily interrupted.

~~(FOUO)~~ We also have a more moderate-paced track for any who might need more than three years to achieve CA certification and complete the G4 Plan. Several branch chiefs are not in favor of back-to-back tours; they need their people between each tour for a full six months or more because they are short-handed and under pressure to keep backlog to a minimum. There are instances, too, where relevant courses cannot be completed in time because of scheduling delays or prerequisites that take time to satisfy.

## COURSES

~~(C-CCO)~~ Three formal courses constitute the bare minimum of what is required to prepare for the CA PQE:

- CA-107 Manual Systems
- CA-110 Cryptostatistics
- CA-123 Shift Registers

P.L. 86-36

The math majors take MA-145 and MA-146 (probability and statistics) in place of CA-110; these longer math courses are a prerequisite to other advanced and relevant math courses. To supplement the over-subscribed CA-123 course at the training school, we have given our own in-house course a number of times to the new arrivals. They all need this particular course, some sooner than others. We have found among the experts in G4 two who have been willing to conduct such a class -- William Mixer of G433, and more recently [ ] of G415. Our instructors coordinate with the training school people and use their course materials and their tests and exams, which are graded by the school; consequently, we can offer the course for credit.

~~(C-CCO)~~ We have also found a willing instructor [ ] of G425, to teach a course in IMP programming. This has proved to be very useful and popular: it was SRO in a conference room the first time he gave it. He has had to repeat it a number of times by popular demand. It is not given for credit, but the lectures and handouts help prepare for any equivalency exam. Most everybody takes either CA-223 or CA-235 [ ] and the math majors all take MA-2T3 [ ] and other specialized math

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

~~SECRET~~

courses. We also recommend CA-261 (diagnosis) and CA-247 (vocoders) to help prepare for the PQE, as well as EA-010 (at the Learning Center) for the Related Fields, in addition to CA-110 and CY-157, and advise MP-160 to those who had no computer science courses in college.

#### INTERNATIONAL ASPECTS

~~(FOUO)~~ Once we were organized and running, G4 was asked to provide cryptanalytic training to an analyst from CSE, Ottawa, who would be sent here for a three-year tour. We were delighted at the prospect of a Canadian connection and charted a special set of tours that would provide both diversification and areas of special interest to his organization. [ ] joined us in July 1983 and is into his fourth tour at present writing. He is taking many courses that we recommended in cryptanalysis and mathematics. He gave a talk recently in the CA-305 series about CSE and his PCS here, and also a G4 SIGSEM talk on a technical project.

#### RESULTS

~~(FOUO)~~ This mixture of courses, tours, and OJT provides a potent brew. As members reach their second anniversary they are eligible to sign up for the PQE. Most everyone does so, having accumulated the necessary 700 points. The results, as of present writing, broken down by exam parts, are given above; parts I and II are the biggest milestones. These results reflect the unusually fine performance of our people.

~~(FOUO)~~ Three members have already received the formal CA certificate, having reached their third anniversary and having completed all the other requirements: 1000 points, PQE, computer program, technical paper, and diversification.

~~(FOUO)~~ The G4 trainees are often in demand for a tour now that their fame has spread. Some of them have had a chance to contribute substantially and in an innovative way to projects while on tour. These efforts have been recognized and appreciated. Our people get their fair share of awards - SSWPs, QSIs, and SPCAs in varying amounts. We are proud of them, and they reflect great credit on G4.

~~(FOUO)~~ Five of our people have been sidetracked onto special projects within G4 for one or two years. This will delay their ultimate completion of the G4 Plan, but their association with these important projects and the experience they gain can only enhance their record. They can always rejoin the Plan; it is conveniently flexible.

~~(C)~~ These newcomers even have a chance to go on TDY for consultation and to attend conferences. Last year, one of our members attended the ACE conference in Princeton; more are expecting to go this spring. Another one of our people, a member of a team of five was included in a TDY trip to IDA to assist in a briefing about their project. Still another had a trip to Bell Laboratories.

#### OTHER CONSIDERATIONS

~~(FOUO)~~ There is no doubt that we have a viable career development program in G4. Implemented some two and one-half years ago, it has grown and developed to fill the needs of our new pre-professionals and to respond to demands of G4's mission. But there have been a few drawbacks that, on the one hand, cause delay and

frustrations for me in arranging tours, and that, on the other, risk a disappointing, unchallenging tour for the individual. For example, interns usually get first chance at training slots (often in short supply) and the better projects to work on -- all for the simple reason that their permanent assignment is made after their first three years, whereas the G4 permanent assignment is made at the beginning upon entering on duty in G4. Furthermore, interns more often than not have a voice in choosing their permanent assignment. All managers, including those in G4, want to attract interns to join them eventually. It is only natural, therefore, for interns to be placed first in tour areas and be assigned the better projects from which to learn new things, whereas the G4 trainees are often expected to contribute their talents, developed elsewhere, and may not have as rewarding a tour. We now know from experience where the better tours for our G4 people are likely to be.

#### CONCLUSIONS

~~(FOUO)~~ The G4 career development program described in this article works very well indeed. Our people are able to compete professionally with graduates of intern programs in the same length of time. They like the idea of a "home" branch and belonging to G4 from the start. They look forward to coming "home" between tours and after completion of the Plan. Through the tours they have experienced a variety of technical problems, and production and management styles, and have made many contacts that could prove useful professionally. Best of all, their "home" branch chiefs want them back ASAP. □

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

CRYPTANALYST <del>(S-CCO)</del>	
[ ]	
We are looking for a dynamic person who can operate in an unstructured environment and achieve results with little direct supervision. The successful candidate will play a leading role in improving A3's ability to produce intelligence.	
Please send your Personnel Summary in complete confidence to:	
<b>A331</b>	<b>A331/3C085</b> <b>963-5246s</b>
<del>(S-CCO)</del>	An Equal Opportunity Employer

P.L. 86-36

~~Secret~~

- ☐ THE
- ☐ CRYPTOLOGIC
- ☐ LINGUIST
- ☐ PROGRAM
- ☐ (u)

- ☐ THE
- ☐ SUMMER
- ☐ LANGUAGE
- ☐ PROGRAM
- ☐ (u)

P.L. 86-36

P16, p16edr@bar1c05

P16, p16lap@bar1c05

~~(FOUO)~~ The Cryptologic Linguistic Program (CLP) was promulgated in 1974 by the director of NSA, General Allen, on the recommendation of the DDO, General Wolff. It is administered by P16, the Language and Linguistics Division of P1, Office of Techniques and Standards.

~~(FOUO)~~ Essentially, the CLP is designed to develop a small but dynamic nucleus of linguists, each with several languages and/or cryptologic skills, in order better to be able to meet changing requirements of production elements, especially during crises. The program strives primarily to develop multilinguists. Participants in the program normally are trained in at least one additional language. The new language is determined by operational necessity and by the language background of the participant.

~~(FOUO)~~ The program runs approximately three years, depending upon the background and experience of the individual participant. In those three years participants rotate through work and training assignments. There are two overseas training opportunities, one in Europe and the other in Asia. Selection for overseas tours depends upon the needs of the overseas organization, the participant's language mix, and timing.

(U) Most participants in the CLP are direct hires with graduate degrees in language or linguistics. On-board candidates who are certified in a language may apply when positions are advertised in the announcement of Competitive Selection Vacancies. Previous selectees have had a wide range of language backgrounds and experiences. Typically, they have had advanced degrees in language, linguistics, or closely related subjects, and usually, they have also demonstrated considerable ability in two or more languages.

~~(FOUO)~~ Since 1974 fifteen participants have completed the program and have been assigned to production elements. Currently there are thirteen participants in the program. □

(U) NSA sponsors a summer employment program for undergraduate and graduate students of foreign languages. It provides them an opportunity to use and improve their skills while sampling language work at the Agency. The experience also offers a "foot in the door" towards a career with NSA upon completion of academic work.

(U) Undergraduate students are eligible to participate during the summer before their senior year, while graduate students may participate any summer prior to completion of their studies. Applicants must have a minimum of 25 semester hours of course work in applied language and pass the Agency's language proficiency test. A major in a language, while desirable, is not required.

(U) Students are given clearances through TSC. Because the processing of applications is necessarily lengthy, eligible students are urged to apply early in the fall prior to the summer for which they seek employment. Interested students should send an SF-171 to the Employment Division, Office of Civilian Personnel. The application and envelope both should be clearly marked, "SUMMER EMPLOYMENT."

~~(FOUO)~~ For the summer of 1985 five students have been hired, three undergraduate and two graduate. Two students have Russian, one has Chinese and Japanese, one French, and one French and German. These students are to be assigned to offices in A, B, G, and W.

~~(FOUO)~~ The operational areas profit as well as the students from having linguists without encumbering billets, particularly during the summer when vacations thin the ranks of linguists. It also allows management to identify prospective hirees on the basis of demonstrated performance. Supervisors interested in having a language student for the summer of 1986 should contact the author at 963-1103. □

~~Secret~~

# COPING WITH CAREER CHANGE (u)



P.L. 86-36

4945

*As part of Career Development Week activities, a panel moderated by John Monroe, now D/Chief, P04, discussed the topic, "Coping with Career Change." The emphasis was on self-help and initiative, and the dialogue centered on both career change and changing jobs. After general discussion by the panel members, the audience was invited to address questions to the panel.*

*Sue prepared the following highlights for dissemination to the field because the topic is particularly relevant to employees in field assignments.*

*During field assignments, individuals are often called upon to develop new skills and to enter new career fields in support of the mission. Such persons sometimes decide to change career fields or to seek certification in still another field. But whether at home or in the field, many people will find the discussion helpful and interesting.*

activity to him. The person may be suffering from a loss of self-esteem and may not feel as competitive, career-wise, as he did formerly. In addition, the individual may have reached that point in a career, perhaps grade level 12 or 13, where there is a heightened selectivity in awarding promotions.

Job satisfaction is important. Self-perceptions and attitudes are important. There are batteries of aptitude tests administered to new employees at NSA which the individual is free to consult at any point during his career and reflect upon if he is considering a career change. On the other hand, it may be time to take advantage of educational opportunities, which are numerous in our agency to prepare for a career change. The key to a career change is: know yourself, know the system, know who can help you, and work on self-improvement.

Do a self-diagnosis. List your strengths and weaknesses. What does it take to get into another job or career field? Networking can be useful. If you have worked for or with another employee who knows your capabilities, you may be able to seek advice or recommendations regarding a new job from that individual. Visibility, familiarity, and the image you project can be important factors in a career change.

Remember, you can't always control career changes. A reorganization, a new mission, or technological change can result in a career change for you. Some of these changes can be a shock to the individual. A new job may not be as good as an old one, but it is still necessary to do the best job you can in the new position, to develop new skills, and to enhance your professional profile so that you will be competitive with contemporaries and promotable.

Remember that a positive attitude and performance are important and can make opportunities available.

P.L. 86-36

The panel members were:

- \*John Monroe, DDO Special Assistant; Moderator
- \*Dr. R. L. James, Chief, Psychological Services, M72
- [redacted] Deputy, D8, Equal Opportunity Office
- [redacted] Technical Advisor to Chief, B
- [redacted] M315

Mr. Monroe introduced the panel and indicated that any point in a career can be a time for reflection. The panel members then elaborated on factors to be considered when an individual is contemplating career changes.

Dr. James: Consideration should be given to the medical aspects of career change during the middle years. It should be considered as part of the crisis triad: life change, family change, and career change. The individual undergoes a great deal of stress during this period and it is necessary for the person to refocus and redefine what is meaningful

P.L. 86-36

Dr. James: A PCS or field assignment may be sought when a lack of job opportunity occurs at HQ. The important thing is to find a job that interests you. Try to assess what your career problem is and solve it. Then pursue a field assignment or any reassignment you desire.

Remember that performance is just one of the keys to getting ahead. Visibility is another key. Visibility can be gained by working on various panels, projects, or task forces where your contribution and ability will be noticed.

Mr. Monroe: Perhaps we can discuss visibility and the value of seeking it out.

Before you seek visibility, you should try to assess whether or not you are a highly competitive person. You should have a strong sense of adequacy to support you as you pursue new career goals or seek visibility.

Some employees try to move to jobs with greater visibility. Moving, in general, is encouraged at this agency, but moving from job to job is not the same as a career change.

Dr. James: Be prepared to deal with stress if you seek visibility. Similarly, stress and frustration can accompany any job change, such as a change from a technical track type of job to a management job. The individual can seek help in such cases. At times, individuals have returned to technical jobs and have successfully gotten rid of stress.

Some agencies automatically rotate personnel to new jobs every two or three years. Some employees are suspicious of change and feel threatened by it. Many times our management initiates change by reorganization, field assignment, technical track career development, Galaxy, and the vacancy announcement system, just to name a few vehicles of change. Management is working to improve the methods used to effect change in the system. There is a real need for change to meet both management needs and the needs of the individual.

#### QUESTIONS FROM THE AUDIENCE

Q: Don't we have diversification, job change, and rotation here at NSA?

Panel: Few of the newly hired employees at NSA have TA or CA skills. These skills, in general, are not available in the market place. NSA hires people with related skills and trains them in specific cryptologic disciplines. With this need, NSA has been developing career paths as a kind of road map for career development which is available for all employees. If you are interested in a specific career field or have an aptitude for it, it is up to you to pursue a job in that career specialty. The means are available here. Decide what you want to do and pursue it.

Q: Are ticket punching and regular moves needed for career advancement? How do these activities relate to the personal crisis?

Panel: In the past, some people have chosen to ignore professionalization. They've said to heck with it. In some

cases, at a later date, an individual may have personally decided to reevaluate this decision, changed his mind, and decided to work for certification, while others continued to resist the career development movement. It is never too late to reconsider, especially once an individual reaches career levels that require professionalization for additional progression. It is always possible to reconsider, especially when performance and skills are top-notch and the employee is highly promotable.

Promotion boards need a weed-out factor. They must consider all qualifications and accomplishments. Factors of concern include: college degree, field assignments, certification, additional education, and staff or operational experience, just to name a few.

The age factor has been raised in career opportunity and promotion cases. Employees who are 40 years of age or older are covered under the EEO umbrella. Hopefully, managers are striving to prevent age discrimination.

If you are not longer being selected or sought for jobs, perhaps you should reflect and consider what you can do to improve your prospects. If you are experiencing stress on the job, confidential counselling is available through psychological services, M72.

The career development office hopes that this panel discussion will help you if you are contemplating a career change. Certainly the experience you gain in a field assignment will be of value to you as you pursue your career. Likewise, self-evaluation, taking advantage of educational opportunities, and application to the Career Development Office for assistance are steps that can help each employee prepare today for a better career at NSA tomorrow. □

#### CA SKILLS ENHANCEMENT PROGRAM (U)

P15

P.L. 86-36

*This article is classified FOUO in its entirety.*

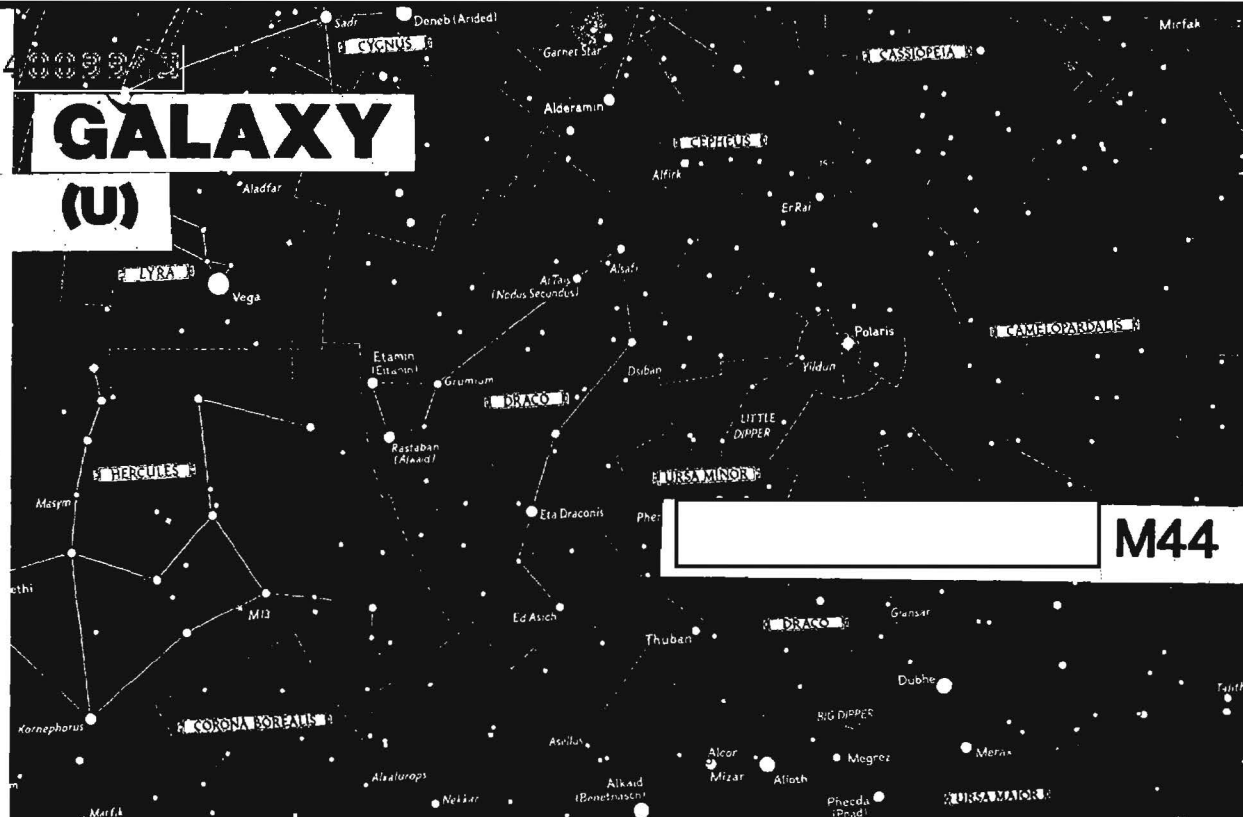
In 1981 P1 initiated a two-to-three-year development program for cryptanalysts and former cryptanalysts who wish to work in the field of manual systems cryptanalysis. The purpose is to identify and cross-train or retrain selected applicants at the GG12-14 level. This program affords participants an opportunity to broaden their experience and sharpen their skills through a series of varied operational assignments and training that are tailored for each individual.

Openings in the program are announced through GALAXY. All candidates must be certified cryptanalysts. For information call [ ] at 963-3957. □

P.L. 86-36

# GALAXY

(U)



For many years Agency personnel have struggled to find direction for their careers once they became professionalized in their field(s) and reached the GS-12/13 grade level. This situation might be labeled the post-professionalization syndrome. When faced with this problem, people take one of several routes. They latch onto a sponsor or mentor who can guide them through the organizational thickets, or they press ahead on their own initiative using the proverbial trial and error method of career management, or they simply do nothing and rely on the "system" to take care of their careers for them. All these career management methods have drawbacks, particularly because they rely heavily on chance rather than on specific procedures.

Agency management has long recognized that there is a void in career development for the post-professionalization population. Finally in 1983 the then Director, Lieutenant General Faurer, formed a task force to establish a mid-level career management program. This task force conceived a program, now known as GALAXY, which would manage assignment and reassignment actions and implement a career development system for all mid-level (GS-13/15) personnel. The task force perceived GALAXY as a bridge between the Professionalization and the Executive/Technical Development programs. One of GALAXY's main objectives is to provide people with developmental assignments and training to prepare them to fill future Agency senior managerial and technical positions.

The GALAXY staff has been working on the assignment aspect of the program for more than a year. In addition, the program is in the midst of its first reassignment cycle and is handling assignments for field returnees in the GG-13/15 category. It has also begun to process assignment of mid-level Agency personnel to field sites for the FY-86 cycle.

It is important to note, however, that the GALAXY assignment procedures are still in a developmental stage and are not yet firmly established. GALAXY and the GALAXY Steering Group, whose members are senior Agency managers, are currently reevaluating the program to

determine the best method of handling the assignment of mid-level personnel.

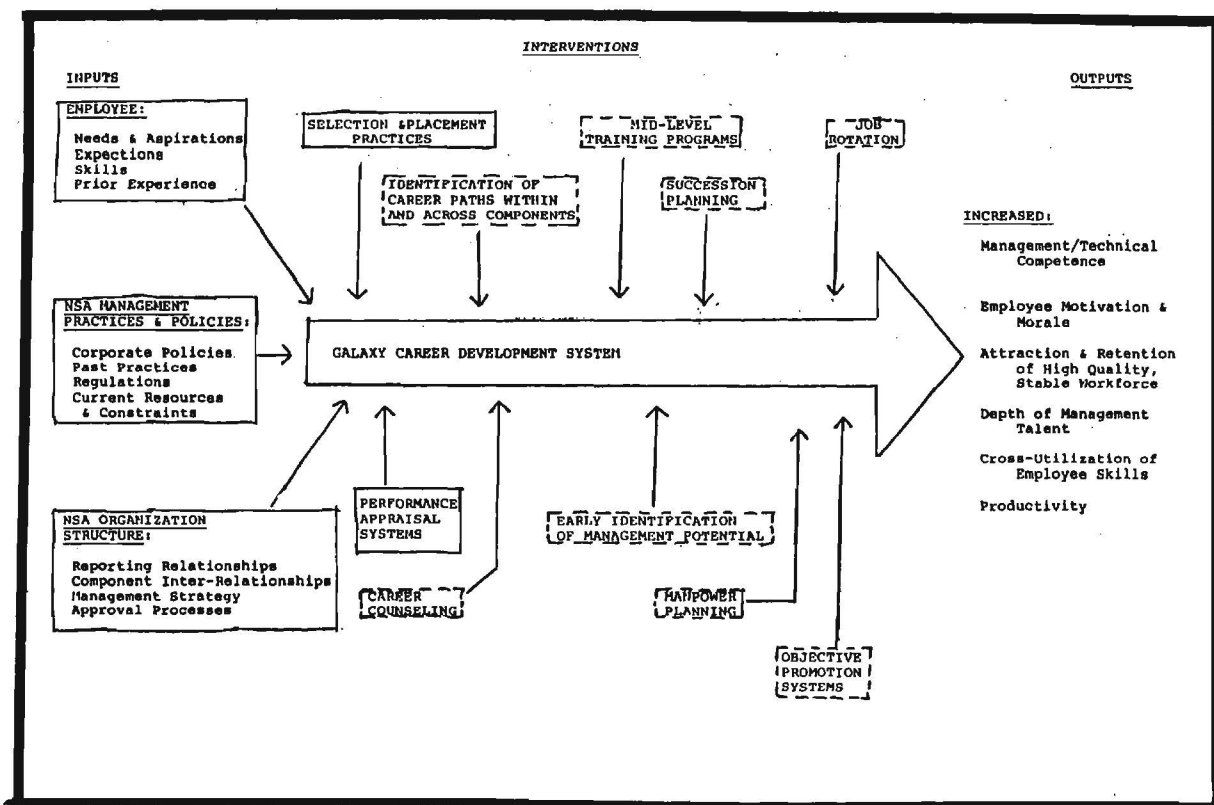
P.L. 86-36

At the same time, GALAXY is moving ahead with planning the second phase of the program, a career development system. As currently envisioned, this phase will include the implementation of career pathing procedures, rotational work assignments, career counseling, advance planning for key positions, and career-related training. The chart depicts how the proposed system will mesh organizational needs and individual aspirations with a variety of career development activities to produce positive results for the Agency and its mid-level workforce.

Basically, we envision a five-part program which will be phased in over a two- to-three year period. To accomplish this, we expect to employ the services of outside professionals throughout the design and implementation process. Once all segments of the program have been installed at NSA, we anticipate that mid-level career development services will be maintained for the most part by the GALAXY staff.

The initial task is to construct a "competency inventory," a database which describes, catalogs, and cross-references basic competency requirements within occupational specialties as well as across specialties, fields, and families of fields. The inventory will maintain the distinction between technical and supervisory skills and knowledges so that career guidance can be provided for both the management and technical tracks. Generation of this competency inventory will depend upon guidance from Agency senior managers, career panels, etc. This presents an excellent opportunity for Agency management to establish guidelines for the future direction of the NSA mid-level population.

The second task is to develop self-assessment surveys which will allow mid-level employees to determine their current competency levels, individual preferences, and motivations. This data can then be used to compare the individual's competencies with the requirements of the position(s) to which they aspire. We will also design a complementary



assessment survey for use by supervisors as a counseling tool in private session with their subordinates. These surveys will assist both the organizations and the individuals to reach their respective objectives in the career planning process.

The next task, to be undertaken simultaneously with the previous one, is to initiate a form of long-range planning to fill key positions. To accomplish this we first need to determine relative growth trends within Agency career fields. Once high growth areas have been identified, competency profiles can be delineated and then appropriate career paths can be outlined for mid-level employees who desire to advance into the high growth areas. These procedures will help to insure that the Agency has sufficient qualified personnel prepared to fill future staffing requirements.

The fourth task is to establish several career management mechanisms to support career planning. One such mechanism is an automated data base which will permit individual career pathing by matching employee competencies with the requirements of position openings and identifying areas for individual development. Another mechanism is a mid-level training package being devised by M4 and the NCS to help the GALAXY population reach their career objectives. A third mechanism is a career counseling center which will contain, among other things, listings of all current position vacancies, jobs identified as rotational assignments, educational and training opportunities, and self-assessment materials. This center will be staffed by GALAXY personnel who will provide counseling, guidance, and feedback.

The fifth and final task is to integrate all mid-level career management and placement support systems in a competency framework. This includes developing

competency-based criteria for entry into higher level Agency positions, as well as criteria to assist employees in choosing between the management and technical tracks. Also at this stage, the competency inventory may require refinement. This will be accomplished by acquiring feedback from managers and non-managers alike as to the comprehensiveness and utility of the program.

All segments of the career development system will be available for use by the GALAXY population as soon as they are completed. The competency inventory will provide employees with guidance on technical and supervisory skills and knowledge requirements for jobs through-out the Agency. The assessment surveys will aid supervisors and non-supervisors alike in determining individual abilities. Planning well ahead to fill key jobs will help to point out trends in future requirements for Agency positions. The automated data base will allow employees to develop individual career planning information. The mid-level training program will help prepare the GALAXY population for higher level positions. And the career counseling center will be the focus for interaction between the GALAXY staff and general population.

In summary, the implementation of a mid-level career development system will help meet future Agency requirements for highly skilled managerial and technical personnel, and will prepare the GALAXY population to fill these requirements. The design of this phase of the GALAXY program is still in its early stages. Therefore, if anyone has any questions or recommendations about this proposed system, we invite you to write, stop by, or call the GALAXY office, M44, Room B6E36, FANX III, 968-7160s or 859-4678b. □



## THE FUTURE OF TRAFFIC ANALYSIS (U)

P.L. 86-36



It is a pleasure to be here and to be asked to think about the future of TA. That's a subject I've been thinking about, in one way or another, for most of my adult life.

I would like to begin by making some predictions about TA twenty years from today. I found a crystal ball and was going to set it up here on the podium for these predictions. However, the guy that owned it couldn't figure out why I wanted it, so I decided it wasn't worth the trouble.

Here are the predictions.

*\* Twenty years from today, people outside the field will be telling us that TA has no future.*

Back in 1946 when I first started, people were quick to tell me that TA was a wartime skill, that it did a fair job during the war, but that it wouldn't be around very long in peacetime. In fact, I can remember not really wanting to be in the field of TA. I was convinced that CA was more interesting, and for a while I did my best to get out of TA so I could work in CA. (Later on, when I got my hands on some actual raw traffic and began to work with collectors, I found that TA was a lot more interesting than I thought.) And people have been predicting the demise of TA ever since. By now it's an old song, but I even hear it today. So it doesn't take much nerve to predict that we will still be hearing that song twenty years down the road.

*\* The highest graded individual in the TA field will be a supergrade, or whatever they are calling them twenty years from now.*

This is another easy prediction. [redacted] got to be a super-grade as a Traffic Analyst, and so did I. I see no reason why other Traffic Analysts can't do the same. If anything, it ought to be a little easier for you, because the Agency is now

more attentive to the technical track than it has been in times past.

*\* Most of the daily front page news in the intelligence community will be provided by TA.*

This is another easy one. We do it now. We have been doing it. It seems an easy projection to say that we will continue. We will still be relying on TA for much of our Information & Warning. There may be some new high-tech wrinkles in the I & W world twenty years from now, but TA has a good track record for reliability and consistency in this area. It is so simple for TA to "reach out and touch" targets to see if they are normal. Even if some good gadgetry comes along, the result will be some sort of partnership between the new techniques and the old reliable methods of TA.

*\* We will still rely on TA for collection steerage.*

It is funny how often this is overlooked in day-to-day operations. And yet, some TA shops could almost pay their own salaries in the savings from more efficient use of collection resources. Signals are getting more complex. Some of today's targets have a lot of money to spend and are modernizing faster than our collection system. All of this will require even more efficiency for collection steerage, and that's where TA has to come in.

This hasn't changed for years, and probably won't over the next twenty. TA people are still "batching" traffic into

homogeneous groups to prepare it for cryptanalytic attack. Ask your favorite cripplies if they would like this to continue. Once cryptanalysts experience good TA support, they become believers; they will ask for it again and again, because they know it helps them to do their own job well.

*\* On Tuesday, the 24th of May, in the year 2005, someone will be heard to say, "My problem isn't a standard TA problem-- we don't use call signs."*

I think I first heard this about 35 years ago when I started working on a radioprinter problem. I really don't think there is a standard TA problem. What we have is one or two problems that are so large, we tend to think of them as standard. But they aren't. Traffic analysts have a large bag of tools, built up over the years. We keep adding to that bag of tools, but we don't throw old tools away. Lately, we've been added some computer tricks to our toolkit, and over the next twenty years, I suspect that other new tools will be developed. We need every tool we can get.

Art Levinson used to say that we were a bit like a man that has lost his wallet on a very dark street. We don't look for it where we think we lost it--in the dark. We look for it over under the street light where we can see. We have to work with what the target gives us. And we use whatever tools are appropriate for the features the target gives us.

This leads me to my last prediction, one I hope does not come true.

*\* Sometime during the next twenty years, your target, or the target you are most interested in, will have a major communications change.*

Maybe the target will find out what we use to exploit his communications, how we do our little magic tricks to produce TA results. Maybe they will have a spy, or maybe some public figure will slip and say too much, or maybe someone will go out and write another dumb book. Whatever the reason, the target will change its system, perhaps at great cost and inconvenience.

First there will be panic and a lot of running around. Then, after things settle down a bit, the traffic analysts will begin to take a look at what the target is giving us to work with. Then they will dip into that big old bag of TA tools, and start building another processing system, a system that will feed the collectors, and the cryptanalysts, and the intelligence community. As they recover the new signal plan, what the traffic analysts find will be new, and maybe some of the tools they use will be new. But it will still be TA. □

## LETTER TO THE EDITOR



~~(FOUO)~~ One of the advantages of being associated with a program such as the Traffic Analysis Intern program is the opportunity to watch the big picture develop. For three years I watched the traffic analysis career field being continually rescued from threats to its survival that came from whatever managerial wonders happened to be exerting influence at the time.

~~(FOUO)~~ While specific to the TA experience, these remarks point out the crucial aspects of organizational life: organizations, agencies, corporations, or whatever, are really people. Hiding behind the various bureaucratic identities cannot disguise this reality. The "health" of the people affects the organization's. When people stop caring, growing, and producing, the organization ossifies and eventually fails.

~~(FOUO)~~ Personal career and organizational development are intimately linked. This Agency has taken vital steps to facilitate career development, thereby assuring its future. This month's Career Development activities are a celebration of this process -- in the past, present and future -- and its meaning for us and the Agency.

## FROM THE PAST



extract from

"The Contribution of the Cryptographic Bureaus in the World War" by Yves Gylden, published in *The Signal Corps Bulletin*, Nos. 75-81, Nov-Dec 1933 - Nov-Dec 1934.

*Mr. Gylden was a well-known Swedish code and cipher expert. The article first appeared in a pamphlet entitled, "Chifferbyråernas Insatser I Världskriget Till Lands," published in 1931 in Stockholm.*

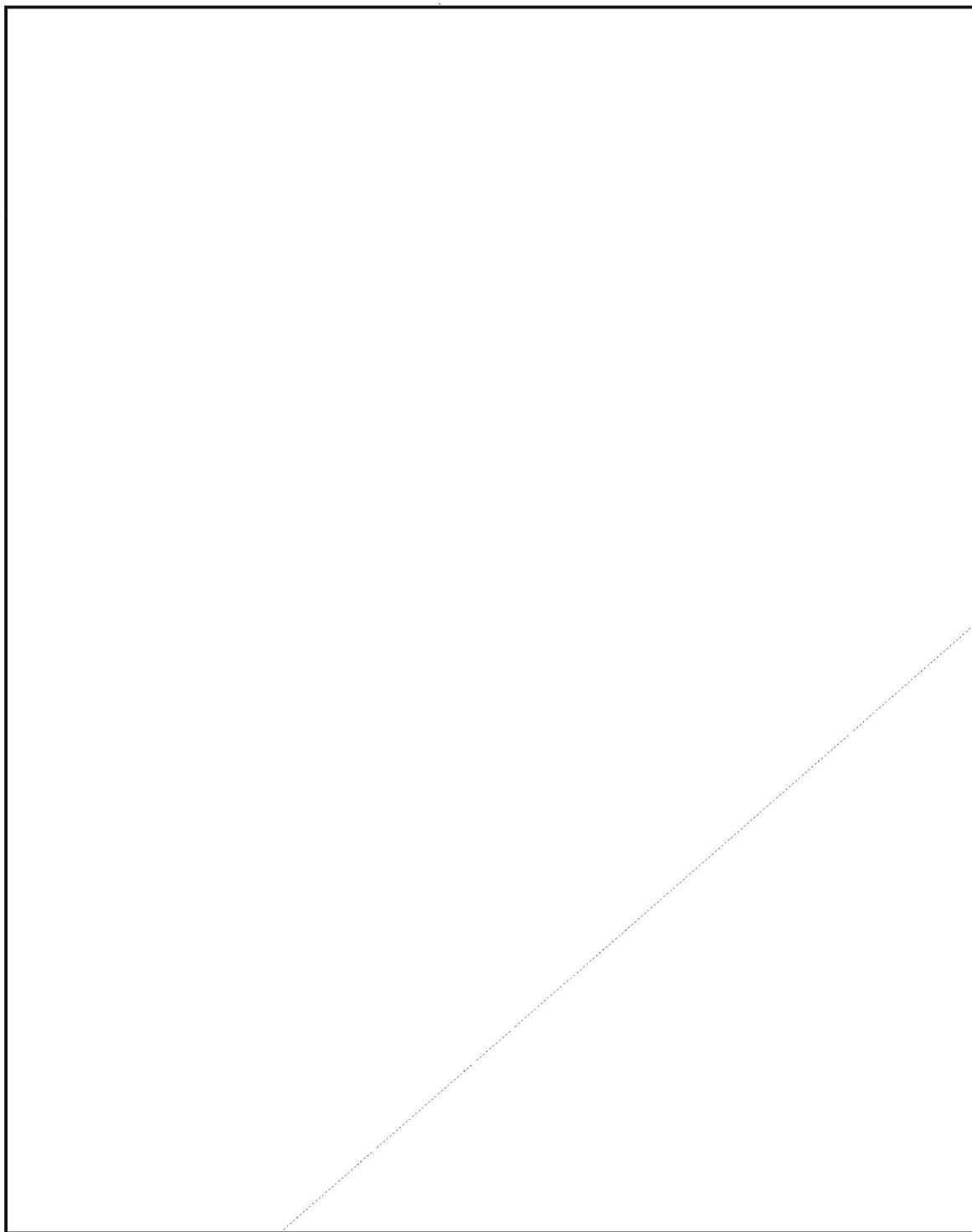
The oldest known cryptographic bureaus were located at Venice under the Doges and at the papal curia in Rome. From 1300 to 1400 these centers were so very well organized that they may in some respects be considered as models even today. Their work included both cryptography and cryptanalysis to an equal degree, and with a logic which even today has no equal in many places, cryptanalysis was placed first for the very logical reason that the person who is best able to solve a cryptogram is able

to grasp the weaknesses of his own systems and work out means for eliminating them.

The requirement for admission to the said Italian bureaus, especially that in Venice, for this reason consisted of the passing of a very difficult examination in the science of cryptanalysis, which was given once a year for applicants satisfactory in other respects.

The technical literature on cryptography of that period also shows a most surprising insight into the problems of cryptography, and we must call attention to the fact that the dissertation [1] on cryptanalysis written in 1474 at Milan by Sicco Simonetta, a cipher clerk, is even today considered greatly superior to all reports prepared by the German school [immediately preceding and during the World War] on the solution of the same cipher system.

[1] *Regulae ad extrahendum litteras zifferatas sine exemplo.*



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

*Reprinted, with permission, from the Spring 1979 issue of the Cryptologic SPECTRUM*

~~CONFIDENTIAL~~**TRAINING****NSA BEGINS INTERN TRAINING PROGRAM**

Nine employees have been selected from 100 applicants to participate in the first Agency Intern Training Program.

Designed to provide a reserve of management-trained personnel from among outstanding civilian career employees, the program began January 31 and ends July 8.

The nine selected received two weeks of orientation and are now beginning rotating work assignments which will take each into from four to seven Agency areas. They meet as a group twice weekly for specialized training in the principles of management and administration.

The selectees are

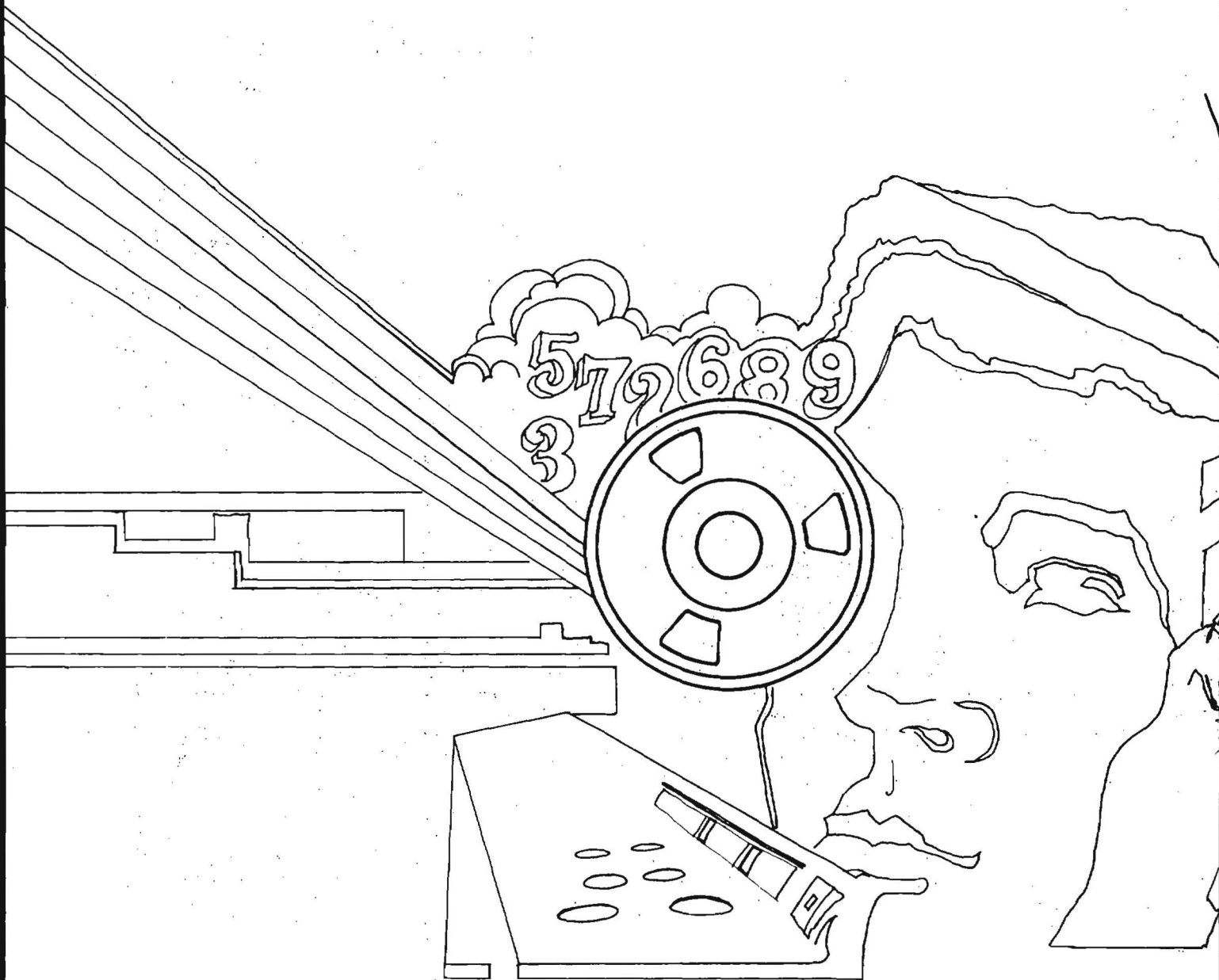
Selection of the participants was handled by Personnel Division, and was based on a written examination, group oral interview, work history, and evaluation by supervisors.

The actual program is conducted by Training Division.

NSA NEWSLETTER, FEBRUARY 1955 ~~(FOUO)~~

~~CONFIDENTIAL~~

~~SECRET~~



~~HANDLE VIA COMINT CHANNELS ONLY~~

~~SECRET~~