~~TOP SECRET~~

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

CRYPTOLOG

SEP-OCT 1985

P.L. 86-36

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

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

CRYPTOLOG

Published by P1, Techniques and Standards

VOL. XII, Nos. 9-10. . . . . September-October 1985

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 equipment, operating system, and 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:
Editor, CRYPTOLOG, P1

EDITORIAL

P.L. 86-36

"Ah, for the good old days ..." NSA writers often sigh when faced with the final chore of their task: marking each paragraph with the appropriate classification. It is a tedious job, and somehow there's always a paragraph or so that takes an unbelievably long time to classify properly.

Well, we've got to do it. One reason can be found in the article on the Freedom of Information Act, beginning on the next page. Everything we write is subject to review. Yes, *everything*. So it does make things easier for the overworked reviewers to scan paragraph classifications than to read carefully an extensive paper that might have but a single classified reference.

And it's no fair trying to play dodgem by overclassifying -- it's also no go; someone will catch it (there are eagle-eyed people everywhere) and make more work for you. Besides, it's hard as it is to get people on the outside to respect our classification system; this will come only when we respect it ourselves. When classification is assigned properly in accordance with the rules, it can successfully withstand challenge.

Occasionally you'll see a notation to the effect that the entire report or article has been classified thus-and-so. That is usually because the classification is the same throughout. If in doubt, do consult your classification officer.

Meanwhile, a true confession: even with all the review CRYPTOLOG undergoes, there's slippage every once in a while, as you will see below.

Ed.

CORRECTION

Please make the following classification changes in the May 1985 issue: Change the classification of page 4 to S-CCO, and change the classification of the fourth paragraph of the article "The Summer Language Program" on page 4 to S-CCO.

UNDERSTANDING THE FREEDOM OF INFORMATION ACT (U)

[redacted] U P.L. 86-36

The Freedom of Information Act (FOIA) affects everyone at NSA. All of us, whether we know it or not, do work which is subject to review - and possible release - under the FOIA. Some of us, sooner or later, may be called upon to review information in response to an FOIA request. Most of us, however, are unaware of the FOIA, have questions about the Act, or would like to understand it better.

The FOIA was enacted by Congress for the principal purpose of broadening access to information about the governmental process. Strengthened by a series of amendments in 1974 and 1976, the FOIA is the primary disclosure statute opening the records of the U.S. Government to public scrutiny. NSA records are subject to requests made under the FOIA and, since virtually all written work product reflecting the official business of the Agency is considered an "agency record," this has the practical effect of subjecting nearly all the written documentation prepared by Agency employees to review and possible disclosure under the FOIA.

BASIC STATUTORY CONTENT

The basic concept of the FOIA requires that an agency, upon receipt of any request reasonably describing the records sought, provide those records to the requester unless the information contained within the records is protected against disclosure by the coverage of nine narrowly drawn statutory exemptions. The exemptions are designed to protect information of particular sensitivity. Thus, there is an attempt to strike a balance between the public's need for information concerning the governmental process and the government's need to preserve the secrecy of certain information compiled in performing its governmental functions.

Exemption 1 to the FOIA protects information currently and properly classified pursuant to executive order in the interest of national defense or foreign policy. Used by NSA to protect classified information from public disclosure, it protects all information properly classified under Executive Order 12356, or originally classified under previous executive orders where the information remains properly classified under Executive Order 12356.

Exemption 2 applies to matters relating solely to the internal rules and practices of an agency. Under this exemption, NSA withholds matters meeting one of two criteria:

- routine, trivial administrative matters in which there is no genuine significant public interest; or
- matters which are "predominantly internal" where, despite the existence of genuine public interest in the subject matter, disclosure would risk circumvention of the

statutes or regulations governing Agency activities.

Exemption 3 authorizes the withholding of information which is protected against disclosure by statute. Federal agencies currently utilize over 130 different statutes to withhold information under the auspices of the third exemption, but NSA principally relies on four different statutory mandates:

- Public Law 86-36 (50 U.S.C. §402 note) - This is the National Security Agency Act of 1959, section 6 of which protects against the disclosure of any information regarding the organization, functions, and activities of NSA; or of the names, titles, salaries, or numbers of employees at the Agency. In asserting the third exemption, NSA cites Public Law 86-36 more frequently than any other statute in protecting both classified and unclassified information concerning the Agency's functions and activities.

- Section 102(d)(3) of the National Security Act of 1947 (50 U.S.C. §403(d)(3)) - This statutory provision authorizes the Director of Central Intelligence (DCI) to protect intelligence sources and methods. As a member of the Intelligence Community, NSA uses this statute in protecting its own sources and methods pursuant to authority conferred by the DCI.

- 18 U.S.C. §798 - A criminal statute, section 798 makes it unlawful to disclose classified information concerning: (a) cryptographic systems, equipments, devices, or designs; or (b) the communications intelligence activities of the United States or any foreign government to any unauthorized person. In requiring that information be classified as a prerequisite to its application, this statute is always used in conjunction with the first exemption.

- 10 U.S.C. §140C - Recently enacted, this statute authorizes the withholding of technical data with military or space application in the possession of, or under the control of, the Department of Defense, if such data may not be lawfully exported outside of the United States without an approval, authorization, or license under the Export Administration Act of 1979 or the Arms Export Control Act.

Exemption 4 protects trade secrets and confidential commercial information. Used primarily in handling requests for information relating to NSA contracts, it allows the Agency to withhold commercial or financial information provided by contractors and other outside entities where disclosure would either impair the Agency's ability to obtain similar information in the future or would cause substantial competitive harm to the company providing the information.

Exemption 5 permits the Agency to withhold information contained within intra-agency or inter-agency memoranda where the information is otherwise protected against disclosure by legal privilege. The privileges most commonly applied are the attorney-client, attorney work-product, and the executive privilege with the latter being used extensively to protect information reflecting predecisional opinions or advice rendered by employees in the Agency decision-making process.

Exemption 6 allows the Agency to withhold information where disclosure would constitute a clearly unwarranted invasion of personal privacy.

Exemptions 7, 8, and 9 are inapplicable to NSA's mission so they are seldom, if ever, invoked. They cover information in investigatory records compiled for law enforcement purposes, information regarding the regulation or supervision of financial institutions, and geological or geophysical information.

MECHANICS OF ADMINISTERING THE FOIA

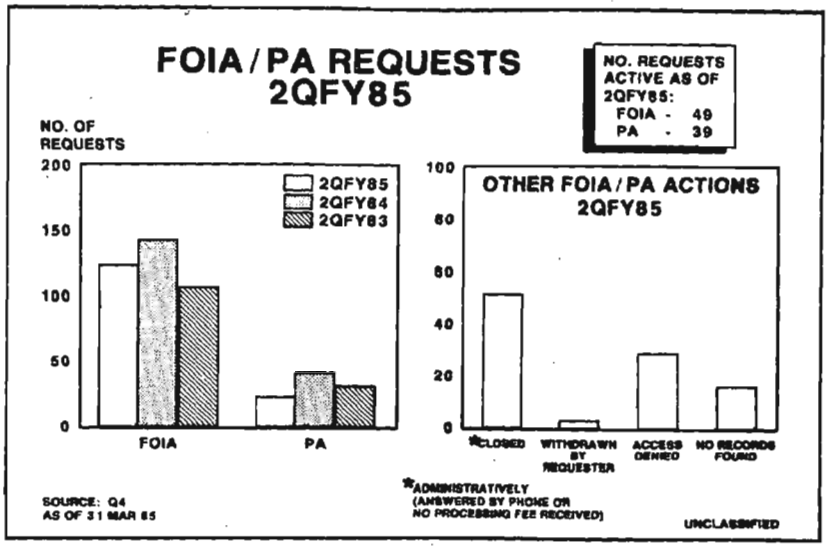
While the FOIA establishes basic principles of disclosure, administering the act is accomplished through procedures developed and implemented by the individual agencies. NSA procedures provide that a requester may seek access to Agency records by a written request reasonably describing the records sought. The Directorate of Policy is charged with administering Agency FOIA activities and the Director of Policy serves as the Agency's Initial Denial Authority; i.e., the Agency official responsible for all initial determinations regarding the releasability of Agency records.

Upon receipt of an FOIA request, the Information Policy Division coordinates both the search for and the review of NSA records responsive to the request. In reviewing records, Agency components must be mindful of the FOIA's requirement to release all "reasonably segregable" information contained within otherwise exempt material. The concept of "reasonable segregability" means that even classified documents must be reviewed to determine whether information responsive to a request can be separated from otherwise classified material and released to the requester. (It is for this reason that marking classified documents by paragraph is now the rule. It greatly faciliates the review process.)

The FOIA provides 10 working days to process a request (i.e., search for, recover, and review responsive documents) and reach a determination regarding the releasability of responsive records. An additional 10 working days is permitted under "unusual circumstances," e.g., the need to obtain records from outlying field facilities, the processing of voluminous records, or the need to consult with other agencies having an interest in the disposition of the records.

STATISTICS ON FOIA AND PA REQUESTS TO NSA, 2QFY85

(U) The following reflects the actions processed under the provisions of the FOIA and PA for 2QFY85 and also compares actions processed for 2QFY83 through 2QFY85. In addition to the actions highlighted below, 108 requests were processed in which the requester received records from which certain sensitive information had been removed. A total of 277 FOIA and PA requests have been received by the Agency through 2QFY85 (versus 330 for the same period last year). To date, 71 of the requests were referred to NSA/CSS by other agencies. The figures do not reflect PA requests by Agency employees which were handled internally by the record holders.



Upon reaching a determination regarding the disposition of responsive records, NSA releases those non-exempt records (or portions thereof), informs the requester, in writing, of the specific exemptions supporting the withholding of those records not released, and advises the requester of the right to appeal any withholdings. Replies to FOIA requests must explain any denials of information, citing the exemptions and statutes invoked.

Under NSA FOIA regulations, a requester has 45 days in which to appeal the withholding of any information. Upon receipt of an appeal, the information at issue in the appeal is reviewed *de novo* by the Office of General Counsel which submits its recommendation regarding the appeal to the NSA FOIA Appeals Authority (the Deputy Director) for a final decision which must be made within 20 days of receipt of the appeal. The FOIA provides that any requester denied information on appeal may sue for release of the information in U.S. District Court.

THE FOIA AND NSA

NSA receives hundreds of FOIA requests annually from requesters seeking information about the Agency, about themselves, and about virtually every topic of interest or concern to any segment of the public.

The most common FOIA requests received by the Agency pertain to commercial information and to current or historical events. Requests concerning particular events have included such subjects as the Cuban Missile Crisis, the attack on the U.S.S. *Liberty*, and the assassination of JFK.

Also common are requests for information about the Agency and for personal records. Many people request information about the Agency as a whole, including the history of NSA and/or pictures of the Agency, or about prominent Agency figures such as the Director or Deputy Director, or about particular Agency projects or developments such as the new building or the Computer Security Center. Copies of the *NSA Newsletter* are also frequently requested.

Some individuals want copies of information the Agency may have on file on them. These personal requests usually are also processed under a sister law regarding personal information, the Privacy Act.

Numerous FOIA requests, however, fall in still other categories. Interesting requests received in the past have included:

- queries about UFO's;

- queries from crypt buffs about purchasing classified crypto-equipment.

While requests may often seem arcane, self-serving, and even frivolous, the FOIA remains the principal means by which individuals can obtain information about the government and its activities directly from the government itself.

COSTS AND CONCERNS

Federal agencies spend millions of dollars administering the FOIA each year. (NSA spent over a third of a million dollars on FOIA last year.) While not designed to recoup all the expenses of FOIA administration, the FOIA does provide for the assessment of fees in conjunction with processing FOIA requests. Fees may be assessed for search and duplication costs, but not for the effort expended by professionals in reviewing documents to evaluate the disposition of responsive information. The FOIA provides further that fees should be waived or appropriately reduced where a fee waiver is sought by the requester and when furnishing the information responsive to the request can be considered as primarily benefiting the general public. The Department of Justice has provided considerable guidance to assist agencies in evaluating requests for fee waivers and ensuring compliance with the statutory policy on fees.

Agencies are concerned about the cumulative amount of information released under the FOIA and the degree of effort and number of employees involved. Companies are worried that their competitive ability may be impaired over time by commercial FOIA releases.

Meanwhile, NSA, like all government agencies, must carry out its obligations under the FOIA as long as the Act is in effect. With regard to commercial information, we must provide releasable information to requesters, while also considering the legitimate concerns of the contractors and vendors. In the case of government records, we must respect the public right to be informed, while simultaneously protecting the national security.

Two things are certain: the FOIA will not go away, and like it or not, the FOIA is the law. □

QUOTE WITHOUT COMMENT

Remarks by Dr. Solomon Kullback, guest speaker, at the Phoenix Society Annual Meeting and Dinner Dance, 27 May 1983, at the Fort Meade Officers Club. Reprinted, with permission, from the PHOENICIAN, Summer 1983.

Sometime in January 1981, I received a telephone call in Florida, from an individual who identified himself as "BAMFORD" of "Houghton Mifflin," writing a book about NSA. My mistake was even to talk to him. Although I cannot now remember the details of the telephone conversation, it was limited to some anecdotes about the period of the thirties.

I did not disclose to Mr. Bamford classified or otherwise sensitive information concerning the activities, organization, and personnel of the NSA. Since I have not been privy to any NSA activities since May 1962, I could not make any disclosure, even inadvertently.

Bamford's reference to me in the Preface is completely unwarranted by the facts and of course was without my permission or knowledge. In his unscrupulous fashion he obviously used me to lend an aura of authenticity to his book. I am particularly distressed by the fact that an AMERICAN CITIZEN and an AMERICAN PUBLISHING HOUSE, apparently motivated by the possible monetary returns, and displaying an obvious bias against NSA, would and could publish a book like *The Puzzle Palace*.

Dear Dr. Kullback,

I recently received a summary of a talk you gave to members of the Phoenix Society. I thoroughly enjoyed the stories of your early days in the cryptologic field; you can be very proud of the legacy left by you and your compatriots.

I appreciate your expressions of support for the National Security Agency and your obvious continuing security consciousness. I can imagine your distress over the misrepresentations made by

Mr. Bamford in his preface, which you referred to in your speech and in your November letter to me. As you noted, he used your reputation to attempt to bring credibility to his book. He did this with other previous -- and some present -- employees to whom he spoke.

Again, thank you for your support.

Sincerely,
Lincoln D. Faurer
Lieutenant General, USAF
Director NSA/Chief, CSS

10 June 1983

LETTER TO THE EDITOR

This is to let people know about a contact I had with James Bamford, author of The Puzzle Palace.

He called me at home one Sunday afternoon to interview me about my lawsuit against NSA for his new book on security practices in government agencies, including those in the intelligence community.

I declined, said that I was still working at NSA, and told him that I had also declined to be interviewed by Mike Wallace on "60 Minutes." He replied that it did not matter, that he had "the entire court record," and that it would be in his book, including my work record which he found "very impressive."

How could he know that? I wondered then, and still do. A summary of my work experience at NSA exists only in a sealed portion of the record, classified TOP SECRET Codeword. It was not to be part of the open record. Nevertheless, on the basis of Mr. Bamford's words and the general tenor of his conversation with me, I am concerned that somehow he did acquire knowledge of the sealed classified record which was a part of my case. An alarming development if so. Or perhaps he was trying to make me believe that, and so entice me into revealing classified information.

These events were duly reported to the proper authorities. But I am assuming that Mr. Bamford is going to describe the case as he said he would and that no effort will be made to prevent him from doing so; a senior Agency official once remarked that such action would be counterproductive.

What must have interested Mr. Bamford is that I won a precedent-setting suit against the Agency under the Privacy Act; I suppose he assumed that I'd be willing to talk to him about it simply for that reason.

The case put on notice those people who, through deliberate intent or just plain ignorance, violate the law. We don't want to see any abuse whatsoever of the constitutional rights of individuals. Nor do we want to see any weakening of our ability to maintain the security practices that are so vital to our National Security. We want to be able to carry out the responsibilities entrusted to us by the American public while at the same time avoiding any actions that have a built-in potential of leading us in the direction of a police state. The task of maintaining the critically important balance between the two is ever-present and difficult. But we can do it without the harmful revelations of Mr. Bamford and others of his ilk.

Albert I. Murphy, E403

LONESOME

Attractive illustrations on Africa (3) seek interesting articles on same. May be scholarly or homespun or straight-from-the-shoulder. Shorties preferred.

Address inquiries to
Editor, CRYPTOLOG, P1

THE WORLD-WIDE SOFTWARE SUPPORT SYSTEM (U)

~~(FOUO)~~ This is an account of the evolution of software support for NSA computer systems deployed to the field. In the 1970's, fielded ADP encompassed over 300 computer systems consisting of over 30 unique computer mainframes and 60 unique software systems. Contractors were used to deploy these systems to the field, while T311 provided software life-cycle support. Documentation standards were being developed and applied to these systems, but it was not unusual to relax documentation requirements to avoid cost overrun.

DEVELOPMENT

~~(FOUO)~~ The PDP-11/70 was chosen because:
- There were many DEC systems in the field, and even more were to be installed;
- It was compatible with the PLATFORM network and the UNIX/PWB operating system.

~~(FOUO)~~ The UNIX/PWB operating system was to provide:
- Network file transfer capability
- Electronic mail capability
- Word processing and editing features
- File security
- A source code control system

(U) The TSSFs were to be headed by an NSA person and staffed with NSA, SCE, and contractor data system analysts. P.L. 86-36

SOFTWARE SUPPORT FACILITIES

(U) With these implementations, Phase I of W2S3 was completed.

REMOTING TERMINALS TO FIELD SITES

~~(C)~~ Direct communication with major fields sites for software support from the TSSFs was the next step. Terminals at these sites were to be interfaced with the theater facility PDP-11/70 software support system via a 600-9600 baud communication circuit. These remote terminals consisted of a Delta Data 7000 terminal and an Anderson Jacobson letter-quality printer.

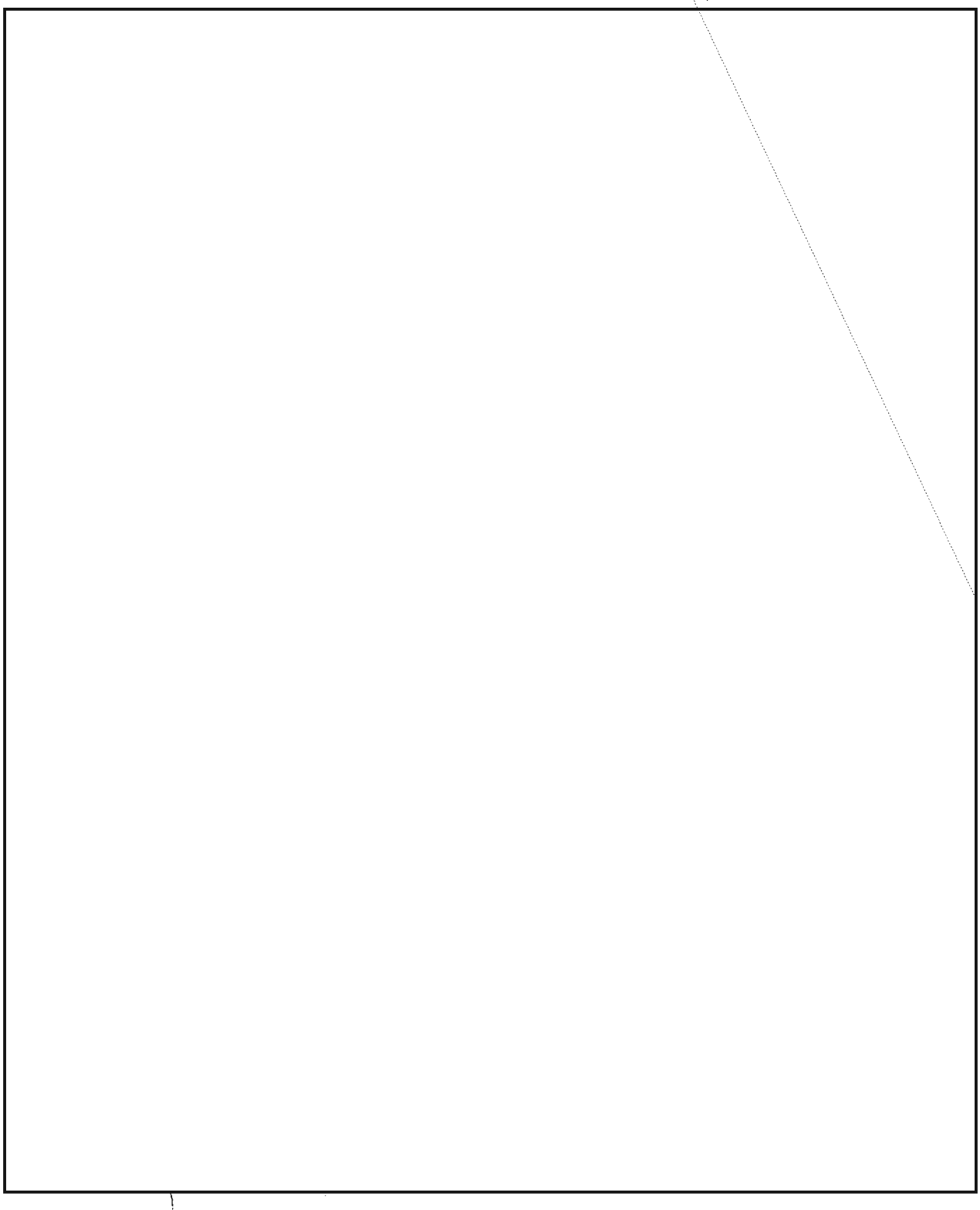
~~(FOUO)~~ The Delta Data 7000 was chosen because it was:
- the T standard terminal for UNIX systems;
- TEMPESTed;

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

 P.L. 86-36

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

THE WORLD-WIDE SOFTWARE SUPPORT SYSTEM (U)



- a "smart" terminal with a TMS 9900 microprocessor and 24K of memory.

(U) Software packages were being developed to take advantage of the Data Delta's capabilities, including:

- a text editor capable of editing a block of 20,000 characters within the terminal;
- a forms package;
- virtual terminal software which allows the screen to be partitioned into four parts, each capable of performing a different function simultaneously;
- TBASIC, for developing software packages to run on the terminal.

SITE SUPPORT FACILITIES

INCLUSION OF THE SCEs

THE FUTURE

(U) Because of the increasing use of floppy disks for input, storage, and software documentation, they have been purchased for the CSSF, ESSF and PSSF.

~~(FOUO)~~ Microprocessors and their firmware are being proliferated around the world. To meet the demands for programmable read-only memory (PROM) firmware support, a portable universal PROM programmer capable of working with over 200 different PROMs is being purchased for each TSSF and SSF. A hexadecimal keyboard is used to make changes and patches to the PROMs. This suitcase device uses 40 to 60 Hz a/c power. It is capable of interfacing with an RS232 port, such as that on a host CPU, a microprocessor development laboratory, or any remote Delta Data 7000 terminal.

~~(FOUO)~~ The need for and use of a microprocessor development laboratory, cross assemblers/compilers on the network, and the configuration management of microprocessors via the PLATFORM network are now being investigated. Much more remains to be done in the continuing development of this new concept in the support of SIGINT systems in the field. But it has already proven to be a cost-effective asset. □

P.L. 86-36

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

book review

THE NEW KGB

by W.R. Corson & R. T. Crowley

Morrow, NY, 1985

P.L. 86-36

Reviewed by [redacted] P13

Editor's note: In order to make it easier for readers to distinguish between the unclassified published material and the classified reviewer's remarks, the latter are shown in **boldface.**

~~(FOUO)~~ The book traces the history of the KGB from its Cheka origins through the OGPU and NKVD periods, with a great deal of fascinating detail, much of it based on FOIA documents. One of the authors was a senior CIA official. **Although cryptology is only a minor theme in the book, it is worth careful reading for it gives a fairly comprehensive picture of the multi-faceted KGB activities. The brutal and clumsy thugs of the past have been replaced by an elite of competent and loyal Russians who are well prepared to control Russia and to penetrate foreign targets.**

(U) Yuri Andropov was a skilled morse code operator and "knew a great deal about the technical aspects of comunications intelligence, including communications security, cryptography techniques, and related technology. In essence, his own familiarity with all aspects of communications intelligence protected him from being overwhelmed by experts in the field ..." (p.434.)

~~(S ——)~~ As soon as Andropov became chief of the KGB in 1968 he put his knowledge of communications intelligence to work in a sustained exploitation of KL-7 traffic from US military forces in Vietnam, using the rotors, keylists and other information obtained in 1963 and later from the US cipher operator Helmich. (p. 342.) **It is well known that in the black markets of Vietnam, current crypto keys were being sold for about $100.**

(U) Andropov also improved the technical competence of the KGB staffs so that they were able to quickly exploit the "Falcon and Snowman" source that provided satellite technical data and crypto keys. (p 376). In the past, the GRU had provided the technical skills, but KGB technical staffing have improved, so that the authors estimate that there are now between 4000 and 8000 KGB and GRU agents in the US concerned with just scientific and technical espionage, concentrated around technical targets such as Silicon Valley and Ft. Meade. (p. 376.)

(U) The exploitation of the Pueblo capture by the KGB in 1968 also seems to reflect Andropov's interest in ciphers and US communications intelligence. (p. 345). The movements of the Pueblo were observed with the help of bar girls and tailors in Yokosuka, and KGB personnel from the Eighth Directorate were moved to the Far East in anticipation of a trap set for the US ship. When the ship was towed in, the KGB team was waiting in the harbor to remove all the equipment and documents for shipment to Moscow, The information taken from the Pueblo gave the Russians a five-year jump forward in their race against the US in cryptography and communications intelligence. (p.346.)

~~(C)~~ **This illustrated the great benefits that can result when the political leadership and the people at the top of the intelligence system can foresee the rich bounty that can come from well-planned "black activities" to augment SIGINT.**

(U) Soviet interest in the cryptography and communications intelligence of other nations has been of long interest. In 1928 the OGPU seized an opportunity to blackmail a disgruntled British Foreign Office cipher clerk who had offered to sell cipher information to their embassy in Paris. They swindled him, but then decided that he could be of further use. In order to locate the clerk in London, an agent deceived the British police into calling the Foreign Office and getting the man's name. (p. 149.) Once he was contacted, they used him to supply cipher information and also to recruit a co-worker in the Foreign Office cipher room. The British Foreign Office was told by an OGPU defector that there was a leak in their cipher room, but the Foreign Office pooh-poohed the notion. When the clerk became uncooperative in 1933 he died an apparent suicide. The co-worker continued to serve the OGPU (KGB) until 1940 when he was identified by an OGPU defector and subsequently imprisoned. The defector was killed in Washington a year later. Through this leak the KGB had advance knowledge of British action and intentions in India, Afghanistan, Persia, and Turkey.

~~(TSC)~~ KGB reaction to the penetration of their ciphers was much more vigorous than that of the Foreign Office. [redacted] After the British police forced their way into the building of the All Russian Cooperative Society in London in 1927 to get proof of Soviet espionage, Prime Minister Stanley Baldwin, a Socialist, stated in Parliament that the British Government had been reading Soviet diplomatic cipher traffic for years, and even read aloud a decrypted message, noting that a group was undecipherable. All this information was published in the parliamentary record, the Hansard. The Soviets immediately changed their diplomatic ciphers worldwide. In a talk at the US State Department in 1975 R.V. Jones said that from that time until 1946 when he left MI6, Soviet diplomatic ciphers were unreadable. (p. 440.) [redacted]

(U) In spite of improvements in Soviet ciphers, an NKVD cipher was read in the postwar era, one that exposed the Rosenberg spy ring. (p. 221.)

(U) The KGB was energetic at compromising and exploiting cipher room personnel of other countries, and took stern measures to keep their own clerks and cryptographers from being exposed to corresponding efforts by foreign intelligence services. Despite this, Igor Gouzenko was able to defect in Canada, taking messages and other materials. Subsequently the controls were tightened even further. (p. 225.)

(U) The KGB recruited low-level military people such as the American NCO Johnson and the British RAF NCO Prime, and maneuvered them into situations where they could supply cryptographic and COMINT information. (pp. 343 and 357.) Sgt. Dunlap at Ft. Meade photographed documents he was supposed to deliver as a messenger and passed them on to the Soviets. (p. 460.) Prime was infiltrated into GCHQ, whence he was able to pass on a variety of information.

[redacted]

(U) One of the outstanding attributes of the KGB is its persistence. It is tireless in going after its targets. The case officers are also good at handling the human element in running agents, combining pressure and rewards. Several appendices give copious details of incidents from the 1920-1950 period that show this combination of ruthlessness, ingenuity and tenacity. And to its own members the KGB is merciless. But in spite of its long sinister history, it is still considered a highly prestigious part of Soviet society, as its "sword and shield."

~~(S-CCO)~~ The authors' closing thesis is that the power in the USSR has shifted away from the Party and the Army, and the KGB will now operate Russia more efficiently than did the ageing and corrupt survivors of the Stalin era. The [redacted]

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

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

BULLETIN BOARD

DEMONSTRATIONS OF [redacted]

~~(C-CCO)~~ The Bookbreakers' Forum on Machine Aids is sponsoring demonstrations of NUTHATCH, a set of bookbreaking programs on the ASTW designed for plain or decrypted codes. The demonstrations are scheduled for the week of 13 January 1986, every day at 0930, in room 2C030. As only six persons can be accommodated at each session, reservations are required. Call [redacted] 963-3045.

PC NEWSLETTER

~~(FOUO)~~ A PC Newletter for G Group personnel is now being published by G331. It lists software for analysis and processing developed in G and elsewhere, and contains helpful hints for both novice and experienced users. For a subscription call [redacted] 963-4524.

FOREIGN-LANGUAGE VIDEOTAPES

~~(FOUO)~~ Videotapes of selected foreign TV programs can be obtained upon request. To inquire about the availability of tapes in your language, call [redacted] 16, 963-1103.

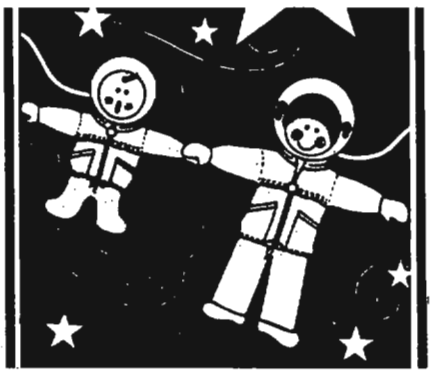
P.L. 86-36

~~SECRET~~

ON THE LIGHTER SIDE

Vera R Filby, E42

There was a new hire named Larking
Who on his first course was embarking.
But he missed his car pool,
(U) So he drove to the School
And was last seen in Overflow Parking.



An NSA linguist named Rease
Could never quite manage with ease
Verb forms in Slovenian
(U) Or Czech or Ruthenian
And therefore he switched to Chinese.

A clever young cryppie named Sue
Had a message that [redacted]
She recovered the keys
~~(S-CCO)~~ With the greatest of ease
But she didn't know [redacted] Do you?

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

There was a reporter named Grotius
Whose grammar and style were atrocious.
But he learned how to spell
(U) And to punctuate as well,
And now he's considered precocious.

When I foolishly tried cryptanalysis
I was suddenly seized with paralysis,
Faced with grids, grills, and matrices,
(U) Vigeneres, generatrices ...
I fear I need psychoanalysis.

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

★★★THE ★ NEW ★ SECURITY ★ LAW★★★

★ *Evert Conder*

★ On 13 May 1950 President Truman signed a new bill designed to safeguard the security of cryptographic and communication intelligence information. Previously, there was only the Espionage Act of 1917: "An Act to punish acts of interference with the foreign relations, the neutrality, and the foreign commerce of the United States, to punish espionage, and better enforce the criminal laws of the United States, and for other purposes."

★ The new measure, Public Law No. 513, is entitled: "To enhance further the security of the United States by preventing disclosures of information concerning the cryptographic systems and the communication intelligence activities of the United States."

★ The safeguarding of this information has always presented a difficult problem. Even though years may pass, publication of techiques or past successes may be dangerous. There is no time limit when security limitations may be safely lifted.

★ The ideal, of course, is to develop your own techniques as far as possible, while trying to keep the other person as uninformed as possible. What he doen't know will not hurt you, while what he learns from you may do great harm. The more secure his lines of communication become, the more difficult your own work becomes.

★ It has always been difficult, even in time of war, for a court to secure a conviction against a civilian accused of disclosing vital military information. Adequate protection, of course, is available for the prosecution of military personnel and other persons subject to military control and the Articles of War. Civilians, however, until now could only be tried under the rather broad Espionage Act mentioned above. The weakness of the Act lies in the fact that (1) pre-meditated knowledge that a foreign government will receive the information, and (2) "intent or reason to believe that it would be used to the injury of the United States or to the advantage of a foreign nation" must be proved. Thus as long as "intent" could not be proved there was no way in which the Espionage Act could be invoked to punish civilians who disclosed military information to unauthorized persons.

★ This fact has been clearly demonstrated several times. In 1931 Herbert O. Yardley published a book entitled: "The Black Chamber" which disclosed certain information about the cryptographic activities of several foreign governments. Although great harm was done, Yardley apparently could not be held to account legally because of the inability of the government to prove "intent to injure." In defense of his actions Yardley maintained he had acted for the good of the country since he was attempting to show how insecure and inadequate our cryptosystems were at that time. A few years later, when Yardley attempted to publish a similar book, it was necessary for Congress to pass "A Bill for the protection of Government records" directed specifically towards gagging Yardley and preventing the publication of his manuscript.

★ Since the end of World War II there has been only one other case where the courts were successful in obtaining a conviction under the Espionage Law. This was the recent case of Judith Coplon. Even here the judge had to charge the jury to consider only two counts: (1) unlawful possession of government records, and (2) conspiracy to commit espionage. The other cases have been tried for perjury. One reason apparently for this is the government's reluctance to chance further disclosures of information which might occur in the court proceeding.★

Reprinted from the
ASA *Review*, Vol. 1. No. 4, July-August 1950

ETYMOLOGIST'S DELIGHT II

Match the borrowed word with the source language.

Edward D. Rockstein, P16, p16edr@bar1c05

"Un draille?"

The etymology of the word "draille" should perhaps be recorded before it has time to fall into obscurity. Before becoming "un draille" it was "un dry." And before that, it was "un dry Martini."

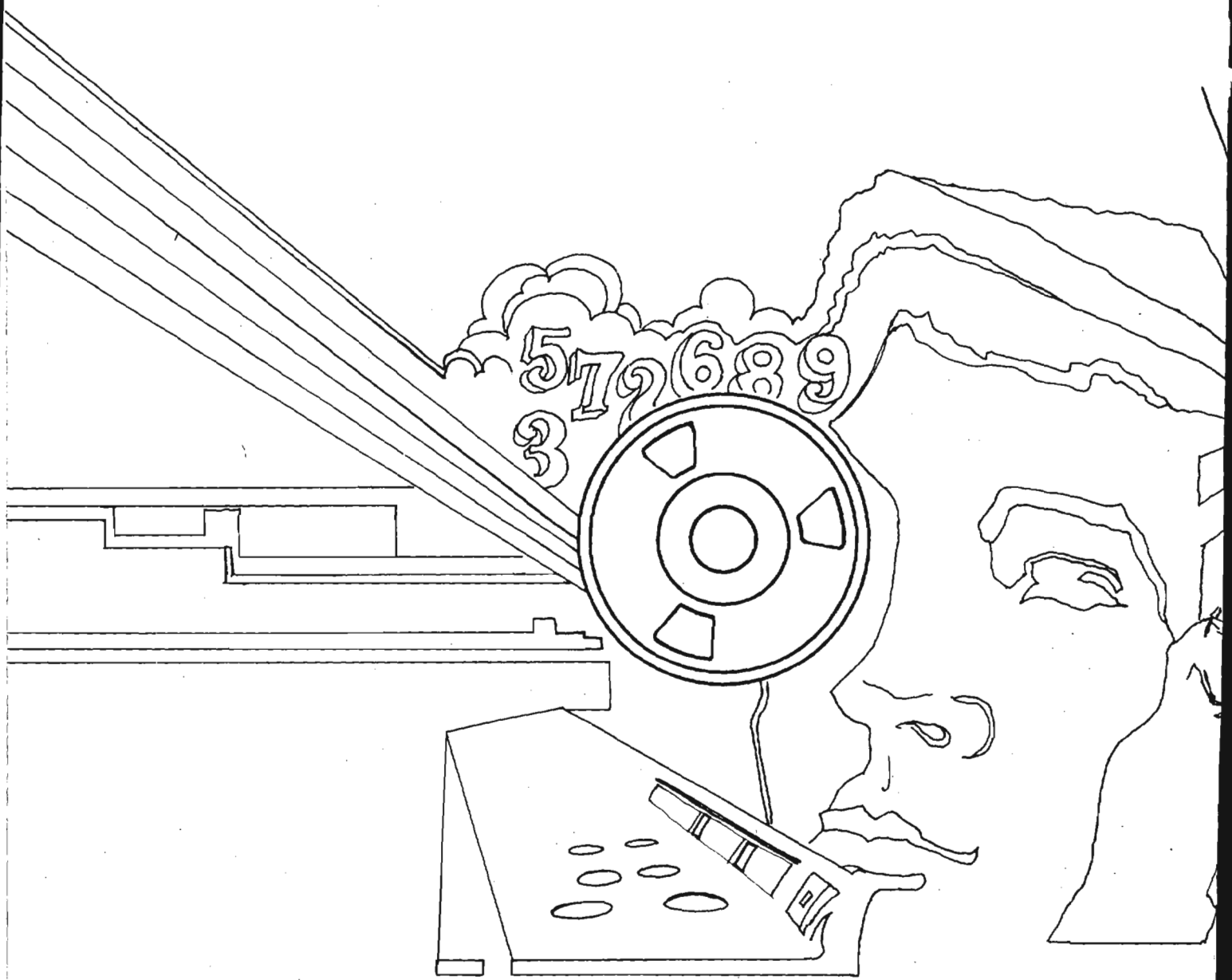
From *Madame Aubrey and the Police* by Hugh Travers

SOURCE LANGUAGES

1. Algonquin
2. Arabic
3. Bantu [Sotho]
4. Basque
5. Breton
6. Celt
7. Czech
8. Dutch
9. Finnish
10. French
11. German
12. Greek
13. Gypsy (Romany)
14. Hindi
15. Japanese
16. Malay
17. Maori
18. Narragansett
19. Norwegian
20. Persian
21. Polish
22. Russian
23. Sanskrit
24. Spanish
25. Swedish
26. Tamil [Telugu]
27. Tibetan
28. Turkic
29. Turkish

WORDS

A. milo (a sorghum)
B. shampoo, bund (a quay)
C. massage, saffron, soda, mortise, lemon
D. go down
E. yoke, Juggernaut, jute, sugar
F. catty (a unit of weight)
G. terrapin, skunk, moose, squash, raccoon
H. tycoon
I. khan
J. yak, zebu
K. drub, casaba
L. menhir
M. jai-a-lai
N. sable, pogrom
O. pistol, howitzer
P. quahog (a clam)
Q. machete, ranch
R. vole, skull, tangle (seaweed)
S. cactus, licorice, skink
T. doodle
U. barnacle
V. pal
W. addle, mink
X. faucet
Y. azure, scimitar, caravan
Z. snorkel, dowel
AA. snook, selvage
BB. kiwi
CC. sauna


5 7 9 6 8 9
3