

DISPOSITION FORM

~~SECRET~~

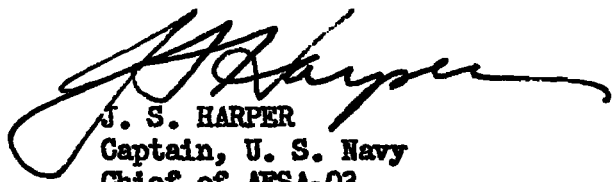
SCAG
file

FILE NO.	SUBJECT	DATE	COMMENT NO. 1
AFSA-00T	Comments by Mr. John H. Howard on the First SCAG Conference	16 July 1951	S. Kullback/60256
TO	FROM		
AFSA-00T	AFSA-03		

1. Mr. Zenner of Teletype could undoubtedly be of assistance to AFSA in its program. When SCAG considers it desirable to expand its membership, Mr. Zenner could be considered.

2. Without adequate means for correlating masses of data and locating available information on the subject, the organization is in effect suffering from loss of memory. The general problem of daily handling and processing raw material is a subject which is under examination by AFSA. We must not expect that such scanning devices will necessarily replace the hunches and guesses of the cryptanalysts. An important aspect of the problem, or at least an important aspect of the problem from AFSA's point of view, is what to coordinate and what to look for, quite a difference from the "library" problem.
record

3. Comments with respect to electronic rotors should have been answered by the recent SCAG meeting.


J. S. HARPER
Captain, U. S. Navy
Chief of AFSA-03

Encl - 1
AFSA-00 memo of 28 Jun 51
w/1 encl

Declassified and approved for release by NSA on 04-02-2014 pursuant to E.O. 13526

~~SECRET~~

~~SECRET~~

Office Memorandum • UNITED STATES GOVERNMENT

TO :

DATE:

FROM :

SUBJECT:

1. Mr. Walt Jenner of Teletype could undoubtedly be of assistance to A FSA in its program. I am not wholly in accord though with the basis of such a contribution as mentioned by John Howard.
2. Machine for correlating masses of data and information are needed but they will never replace the insight

~~SECRET~~

Office Memorandum • UNITED STATES GOVERNMENT

TO :

DATE:

FROM :

SUBJECT:

hunches and guesses of the cryptanalyst.
The problem is what to record and what
to look for - quite a difference from
the "Library" or "Cataloguing" problem.

3. The electronic rotor phase will be answered
by the 10 July meeting

~~SECRET~~ HKu usach

STANDARD FORM NO. 64

Office Memorandum • UNITED STATES GOVERNMENT

TO OBAL

DATE 16 July

FROM OBA

SUBJECT: John Howard's ltr of 6/6/51

1. Suggests get Mr. Walter Zenger, of TTI, to help on printers and on problems of intercepting, forwarding, editing, and punching large masses of data into tapes or cards.
2. Mechanized aids for the organization, correlation, storage and retrieval of cryptanalytic and intelligence data:

Howard feels this area is neglected.

" believes Prof. Berry of MIT is helping CIA on a phase of this problem. Believes AFSA can help
CIA

Office Memorandum • UNITED STATES GOVERNMENT

TO :

DATE

FROM :

Cent Developments -

SUBJECT:

*Keysort**IBM cards**Bush Paper Selector**CNA Microfilm Selector**Calvin Moores Lato coding**Some special IBM developments**Sponsored by Am. Chem Soc. Punched
card Committee headed by Prof Perry*

Office Memorandum • UNITED STATES GOVERNMENT

TO :

DATE:

FROM :

3. Electronic Rotor

SUBJECT:

Howard believes brute force representation by a 1,000 point matrix is a poor & fruitless solution. Doubts that Afa has gotten beyond this point. Situation needs a "really hot idea" -

Suggests a symposium of 10 or 20 participants be given the problem - Possibly someone could come up with an idea -

4. Pse prepare 03 comments to OO T.

\$

From: AFSA 34

TO: AFSA 03

Subject: SCAG, John Howard's Comments on

1. The subject of printers is an extensive one, and one which AFSA needs to know all that can be known, both for intelligence and for production purposes. Zenner sounds like a valuable adjunct to SCAG.

2. The retrieval of information is a subject close to my own heart. As AFSA grows it suffers more and more from loss of memory. If it were magically possible to correlate and retrieve all our information we could do with 10% of the present personnel and do much better to. The design of NOMAD is aimed at a special version of this type of problem, that is in which the information is generated and modified in the course of the solution.

A serious difficulty in realizing this magic is that of getting the raw data into a mechanical medium, such as I.B.M. punched tapes. We are making only slow progress in this problem.

Some of the versions of the retrieval problem are not amenable to NOMAD. These include the traffic analysis problem, and the intelligence digestion of AFSA 25. There are methods known for dealing ^{with} such problems, but unfortunately they are good only for files with relatively constant data. Our files continually change.

Some of the impressive achievements of AFSA have in the past been due to astounding feats of mental correlation on the part of some of our workers. For example, people have remembered seeing cipher digroups, ^{elsewhere} and on locating and comparing the two have verified that they were busts. As the data gets larger this becomes increasingly rare.

e3. An wired wheel representation,
no comment.

W. Campagne

~~SECRET~~

AFSA-00/wm
Serial:~~SECRET~~

28 JUN 1951

~~SECRET~~

Mr. John H. Howard

PL 86-36/50 USC

Dear John:

I am very thankful for your letter of 6 June, and particularly pleased to learn of your favorable reaction to the first SCAG meeting.

I have made note of your high opinion concerning Walt Zenner of Teletype in connection with printers. I shall discuss the possibility with Captain Wenger of utilizing him as you suggest. From what you have said, I agree that he might be of real help in advising us. I have also made note concerning Zenner's brother at Armour Institute who is the expert on magnetic recording.

Under separate cover I am returning several pamphlets and papers which you so kindly sent me. I have kept the copy of Mr. Coleman's talk on "Electronics for Business -- Luxury or Necessity?". I read his paper this morning with considerable interest and enlightenment. Many thanks to you for sending me all of that material.

In order to tie in more closely the common interests of AFSA and CIA, I am arranging to have a permanent representative from CIA meet with SCAG. At this time, I do not know who will be nominated by CIA, but I have requested that he be technically qualified to participate in SCAG discussions.

In order to get started on the group in SCAG to form a "Board of Visitors", I am submitting the nomination of Rear Admiral Joseph R. Redman, U.S. Navy (Retired), to the Chairman, Research and Development Board, with a request that he be invited to become a member. I shall endeavor soon to nominate some other men to serve in this capacity also, and very much appreciate the list of names you previously sent me. I do not believe we will be able actually to organize the Board for an inspection tour of AFSA while I am here, but I would think we could get started on that matter early in the fall. In any case, I intend to mention it for discussion at the next meeting of SCAG.

I am having extracts of your letter of 6 June typed in order to distribute the important ideas which you have presented to those persons in AFSA who are in a position to consider them seriously with a view to action, as may be practicable.

~~SECRET~~

AFSA-00/wm
Serial:~~SECRET~~

28 JUN 1951

~~SECRET~~

I am looking forward to our next SCAG meeting, which will be the last one I shall be able to attend. I hope to have SCAG firmly established after that meeting and the various members ready to assist AFSA in various important ways. I am sure that SCAG is a very worthwhile idea and personally have no doubt that its members will contribute a very great deal in the future.

With all good wishes, I remain

Sincerely yours,

EARL E. STONE
Rear Admiral, U.S. Navy
Director, Armed Forces Security Agency

Copy to:
AFSA-00B
AFSA-00T
AFSA-03

This document contains information affecting the national defense of the United States within the meaning of the Espionage Laws, Title 18, U.S.C., Sections 793 and 794. The transmission or revelation of its contents in any manner to an unauthorized person is prohibited by law.

RADM Earl E. Stone/wm/28Jun51
AFSA-00, Ext 60528

~~SECRET~~

~~SECRET~~

AFSA-00/wm

~~SECRET~~

28 JUN 1951

MEMORANDUM FOR: AFSA-00B
 AFSA-00C
 AFSA-02
 AFSA-03 ←
 AFSA-04

SUBJECT: Comments by Mr. John H. Howard on the First SCAG Conference

1. The enclosure is a partial copy of a letter I received from Mr. Howard. Please consider with a view to appropriate action, as may be practicable and desirable.
2. Forward any comments on this matter to AFSA-00T for coordination.

Earl E. Stone

Enclosure - 1
 Partial copy of ltr from
 Mr. John H. Howard to
 DirAFSA

EARL E. STONE
 Rear Admiral, U.S. Navy
 Director, Armed Forces Security Agency

Copy to:
 AFSA-11
 AFSA-00T

~~SECRET~~

~~SECRET~~

June 6, 1951

~~SECRET~~

Admiral E.E. Stone, Director
Armed Forces Security Agency
Department of Defense
Washington 25, D.C.

Dear Admiral Stone:

I want to thank you for Monday and Tuesday of this week -- two days that will be the highlight of my life for many years to come. I have always been proud of "my old outfit", but not as much as I was this week when the importance of the work you are doing was reaffirmed, and the tremendous progress you have made in the past few years was evident. I was particularly impressed by the presentations by Captain Wenger, Andy Gleason and Frank Raven. I was fearful before I came that the advisory group might be difficult to manage because of its mixture of engineering, mathematical and management people, but it certainly went smoothly and was one of the best managed affairs I ever attended. In any case, I, who might be expected to be somewhat biased, was impressed and I know from personal reports that men such as McPherson and Shannon were overwhelmed.

A number of points occurred to me during the conference but I will mention only a few here. I was quite interested in Frank Raven's presentation on the reconstruction of the printer characteristics and its tendency to stutter. At that time my thoughts turned to Walt Zenner of Teletype who probably knows more about printers than anyone else in the world.

I believe that he has designed and built literally hundreds of experimental printers of all types -- wheel, basket, sector, etc. I wondered if he might not be of real help in studying the evidence and helping reconstruct the actual machine. I believe he had a lot to do with the design and production of the E.C.M. and other machines of this type so he should be a real expert on wired-wheel cipher machines. In addition, he developed many of the new Teletype products in operation (such as the Model 28 high speed system) or still under development (such as the teletype tape punch Joe Kachus has on loan that punches 60 columns per second). Consequently, he might be of real help in advising your activity regarding its massive problem of intercepting, forwarding, editing and punching the large masses of data into tapes or cards.

~~SECRET~~

COPY

~~SECRET~~~~SECRET~~

Zenner impresses me as having the type of mind that would take naturally to cryptanalytic problems. He is more of a planner and thinker than a production engineer. He used to be the "Engineer of Product Development" (same as Chief Engineer) but has been promoted to a long-range planning job having the title "Development and Research Consultant". Mr. M.T. Goetz (who is obviously more of a production driver) is now Engineer of Product Development. The way I read the situation at Teletype, Goetz is very busy and couldn't do a job for you, whereas Zenner has been relieved of most administrative responsibility and might be free to spend considerable time on your problems. Dave Whitelock knows these men much better than I do and you might want to talk to him -- but I do know he has a very high regard for Zenner. Incidentally, Zenner's brother is the man at Armor Institute who is the expert on magnetic recording and who might be associated with Project NCMAD.

My second point has to do with mechanized aids for the organization, correlation, storage and retrieval of cryptanalytic and intelligence data. It has seemed to me for some time that here is a neglected area in which real progress might be made and in which powerful tools for use both in AFSA and CIA might be developed. I have been following the work of Professor Perry at MIT for a number of years and I suspect but do not know for sure, that he is now making a study for CIA regarding coding and organization of intelligence information. He is not strong on mechanization aspects, in my opinion, and I am wondering if AFSA might not take the initiative regarding the development of equipment for both itself and CIA because of its vast experience in the development and procurement of equipment of a similar nature. At least AFSA might offer its services to CIA in an advisory capacity if that agency intends to launch into a development program. I am being frank with you in this secret letter because I realize you may or may not want me to bring up this subject in the SCAG committee because of AFSA-CIA relationships (about which I have no knowledge).

In order that you and your staff may have an idea of what I have in mind, I am enclosing two reprints which I would like to have returned when convenient. Past developments have followed along the lines of Keysort (edge notch) and IBM punched cards, the Bush Rapid Selector, the ERA Microfilm Selector, Calvin Moor's Zato coding, and some special IBM developments that I believe Dr. Ezechus has seen at Poughkeepsie. The latter was sponsored by the Am. Chem. Society Punched Card Committee under Professor Perry. (See page 755 of enclosed reprint). I

~~SECRET~~

~~SECRET~~

believe IBM has this development working satisfactorily but will not make a move toward announcing it publicly or making the machines because of their special nature. A news release in the Chemical and Engr. News of October 30, 1950, page 3789, says that IBM has developed a new type of machine in conjunction with the Committee for Scientific Aids for Literature Searching, that it was hoped that a demonstration would be held in October and that it would be of two types; i.e., (1) Searching of published papers and (2) Correlation of data. I hear that a closed demonstration was held before the committee but that IBM hasn't budged since because of policy involved.

You may not be clear as to what this information storage, correlation and retrieval has to do with AFSA's problems in general and the major SCAG problem in particular. It is this, in my thinking. As your people get further and further into a problem they accumulate a large mass of data, information, hunches, busts, etc. Much of this mass of data is uncorrelated -- and it is the genius of someone like Frank Raven that can absorb multitudinous incidental facts -- make shrewd guesses and somehow put various apparently unrelated pieces of information together and come up with the answer. As we saw the other day, even the individual operating habits of enemy communication clerks may be studied and used to advantage. If you accept this as a fair statement of the problem, then you may see my interest in mechanized aids to help with this process -- and present punched card and electronic equipment you now have are not appropriate for this job. It seems to me that this is a general problem facing both AFSA and CIA that might well be attacked on a broad basis by SCAG -- the mathematicians considering methods for classifying and coding intelligence information (and later its semi-automatic correlation) and the engineers consider ways of mechanization of the processes developed by the mathematicians.

I would like to point out the large amount of work that has been going on in the library field along this line. Unfortunately, it is a very very difficult job to classify all human knowledge as we so bravely started out to do in the Bush Library Selector, but it may be practical to classify intelligence data about specific cipher machines and their usage for cryptanalytic purposes.

My third point has to do with the problem of the electronic rotor. I have thought about this problem for many years without success. I have come to the conclusion that brute force representation by a 1,000 point matrix (or so) is a poor and fruitless solution. I couldn't tell from the presentations the other day if AFSA had gotten beyond this point but I doubt it. This is a situation which needs a really hot idea -- the application of some physical phenomenon to simulate the action of the rotor

~~SECRET~~~~SECRET~~

directly. If this is a real problem for which you do not see a solution as yet, I think it might pay to organize a symposium of 10 to 20 trusted scientists from various backgrounds and describe the need for high speed rotors to them. Such a disclosure need not go into cryptanalysis and might be kept on a CONFIDENTIAL or SECRET level. Maybe one of these men will draw on some unrelated experience in atomic energy, optics, microwaves, etc. -- bridge the gap and come up with a new basic concept. I don't know whether I think so much of this last idea because it is such a gamble -- but if the situation becomes desperate, it might be worthwhile.

Sincerely yours,

/s/ John H. Howard

~~SECRET~~