~~SECRET~~

AFSA-00/mm

~~[redacted]~~

28 JUN 1951

MEMORANDUM FOR: AFSA-003
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
Rear Admiral, U.S. Navy
Director, Armed Forces Security Agency

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

Copy to:
AFSA-11
AFSA-00T

~~SECRET~~

~~SECRET~~

~~SECRET~~

314 Wyndmoor Road
Springfield, Del.Co., Pa.
June 6, 1951

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 Tenner 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 Zachus 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~~

Enclosure (/) 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. Coetz (who is obviously more of a production driver) is now Engineer of Product Development. The way I read the situation at Teletype, Coetz 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 NOMAD.

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 SCAC 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 Rush Rapid Selector, the ERA Microfilm Selector, Calvin Mooer's Zato coding, and some special IBM developments that I believe Dr. Eachus 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

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 SCAC 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 SCAC -- 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

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