

MEMO ROUTING SLIP

NEVER USE FOR APPROVAL, DISAPPROVAL, CONCURRENCES, OR SIMILAR ACTIONS

1 NAME OR TITLE	INITIALS	CIRCULATE
ORGANIZATION AND LOCATION	DATE	COORDINATION
2 <i>Comme came 16 July 1951</i>		FILE
		INFORMATION
3		NECESSARY ACTION
		NOTE AND RETURN
4		SEE ME
		SIGNATURE

REMARKS

P. 8 - 1st term } military director in
 4 yrs } civilian deputy
 (also p. 125)
 " p. 126 - [pro]

9 - Ex Agent to manage for the 6 interests
 depts & agencies for production,
 security and distribution
 Comit + to manufacture, safe-
 guard and distribute the nation's
 own crypto systems.
 [But p. 7: "This responsibility should not
 affect respons + auth of other agencies
 in re evaluation and dissem of the Comit
 prod received from AFSA"]
 [Same on p. 122]

FROM NAME OR TITLE _____ DATE _____

Declassified and approved for release by NSA on 10-16-2014
 pursuant to E.O. 13526

should be limited to civilians, because we are impressed by the testimony given by many witnesses as to the misuse of family duty by the Service Orgs in the field with AFSA org. and ops by rotating 0's from AFSA into field pos + then "back again. ... On the other hand, it would be a major mistake to limit the senior positions to officers, because it is of the greatest importance to encourage civilians to make careers in the Command field by clear demonstration that senior positions will be available to them if their talents merit promotions."

"One cause [high turnover rate among AFSA employees], emphasized by informed witnesses, appears to be that many of the air corp believe that no matter how long they work or how expert they become, the top positions in the divisions will generally be filled by off. pers of less experience and pay than they."

MEMO ROUTING SLIP

REF ID: A4146482
NEVER USE FOR APPROVAL, DISAPPROVAL,
CONCURRENCES, OR SIMILAR ACTIONS

1 NAME OR TITLE	INITIALS		CIRCULATE
ORGANIZATION AND LOCATION	DATE		COORDINATION
2			FILE
			INFORMATION
3			NECESSARY ACTION
			NOTE AND RETURN
4			SEE ME
			SIGNATURE

REMARKS

P. 127a - "On the mil side, a corresp study should be initiated on the question of extending to the Army and to the Air Force the policy now in force in the way of making Comint a career assignment, ~~and~~ ..."

P. 130 - "We have concluded that the problem should be resolved by the issuance of a pres. memo designating the DGD as the ex agent of the GPO for the prod + disssem of Comint for the benefit of the Sucas & the air agencies & depots for the prod, security and distrib of our own C2C systems"

FROM NAME OR TITLE	DATE
ORGANIZATION AND LOCATION	TELEPHONE

MEMO ROUTING SLIP

NEVER USE FOR APPROVAL, DISAPPROVAL,
CONCURRENCES, OR SIMILAR ACTIONS

REF ID: A4146482

1 NAME OR TITLE	INITIALS	CIRCULATE
ORGANIZATION AND LOCATION	DATE	COORDINATION
2		FILE
		INFORMATION
3		NECESSARY ACTION
		NOTE AND RETURN
4		SEE ME
		SIGNATURE

REMARKS

P120 - "There is inadequate attention to the level up of career officers + need opp for that advancement of civilians which is nec to the bldg up of a strong + permanent civilian staff. The increasing complexity of the tasks before AFSA demands the continuity which will result if more of its key persons are career experts."

FROM NAME OR TITLE	DATE
ORGANIZATION AND LOCATION	TELEPHONE

MEMO ROUTING SLIP

NEVER USE FOR APPROVALS, DISAPPROVALS,
CONCURRENCES, OR SIMILAR ACTIONS

1 NAME OR TITLE	INITIALS		CIRCULATE
ORGANIZATION AND LOCATION	DATE		COORDINATION
2			FILE
			INFORMATION
3			NECESSARY ACTION
			NOTE AND RETURN
4			SEE ME
			SIGNATURE

REMARKS

The 4 Encls loaned to
Col. Hetherington about
2 April, 1952

FROM NAME OR TITLE	DATE
ORGANIZATION AND LOCATION	TELEPHONE

Serial: 00087

~~SECURITY INFORMATION~~
~~TOP SECRET~~
~~TOP SECRET - SECURITY INFORMATION~~

2 APR 1952

MEMORANDUM FOR MR. GRANT MANSON:

SUBJECT: Reports by Flicke

1. The contents of the three enclosed TICOM documents, written as "home work" by Wilhelm F. Flicke, a former top-level German COMINT specialist, may be of interest to the members of the Brownell Committee.

2. A brief biographical note on the author of the enclosures is also attached. You will gather from it that his extended experience in the COMINT field qualifies him to write with considerable measure of authority and his comments are well worth study.

ENCLS-4

1. DF 268 Copy No. 27
2. DF 219 Copy No. 32
3. DF 249 Copy No. 52
4. DF 219-G, Copy No. 31

WILLIAM F. FRIEDMAN
 Consultant

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 the revelation of its contents in any manner to an unauthorized person is prohibited by law.

W.F.Friedman/eby/2 April 52
 AFSA-00T/Rm19232B/Ext. 60493

See also Public Law 513,
 81 Congress second session

~~TOP SECRET~~

00T - Comrade Copy

~~SECURITY INFORMATION~~~~TOP SECRET SUEDE~~~~SECURITY INFORMATION~~C O P Y

AFSA-23

Necessity of Plain Text in Cryptanalysis

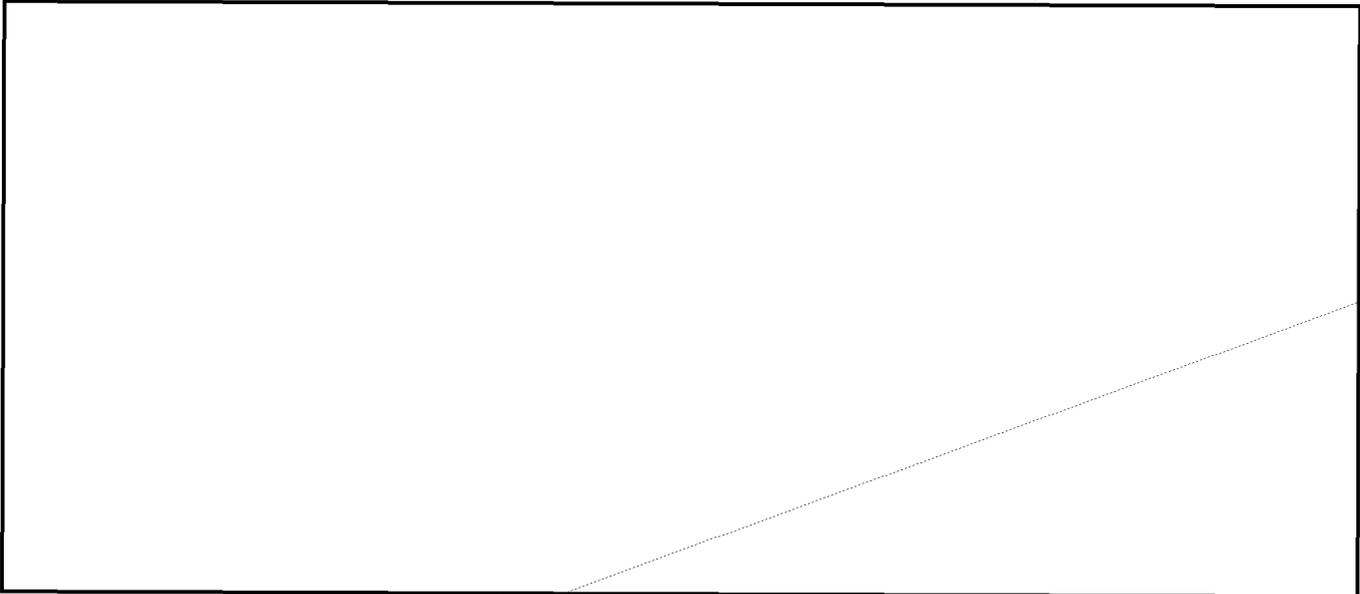
AFSA-2303

28 February 1952

1. All sections of AFSA 230 are reading some of the cryptographic systems of the countries with which they are concerned. The availability of plain text material has been found invaluable in many cases; on several occasions it has led to solution of new systems. All cryptanalysts and translators will testify to the necessity of bringing together all related data for the optimum exploitation of communications intelligence. Specific examples are cited below.

2. A cryptographic system is not solved in a vacuum nor in an ivory tower of abstract mathematics. The basis of operations at AFSA, namely that one operating unit shall process the traffic of a specific country, cipher and plain text, has proved its value. This method has involved the correlation of all available information, historical background, current collateral, plain text and cipher traffic, all of which are essential, not only in cryptanalytic solution but also in scanning, priority assignment and translation of communications intelligence. It is a basic principle in analytic research that all available pertinent materials of a specific, homogeneous type be studied together. The production of communications intelligence is no exception. In an analysis of messages dealing with a specific topic all available messages should be included in the study; the original external form of such messages, whether plain text or cipher, transmitted by teletype, Morse, voice or some other medium, is an incidental feature which has no relevant bearing on the methods of producing COMINT. AFSA's mission is the production of communications intelligence; if AFSA is to carry out its mission, plain text and cipher must not be separated.

3. In addition to the broad requirement for study of plain text in cryptanalysis, the following are specific instances of solution of cipher by use of plain text in AFSA-233:



~~TOP SECRET SUEDE~~

~~TOP SECRET SUEDE - SECURITY INFORMATION~~

C O P Y

AFSA-23

Necessity of Plain Text in Cryptanalysis Cont'd
AFSA-23C3 28 February 1952



~~TOP SECRET SUEDE~~

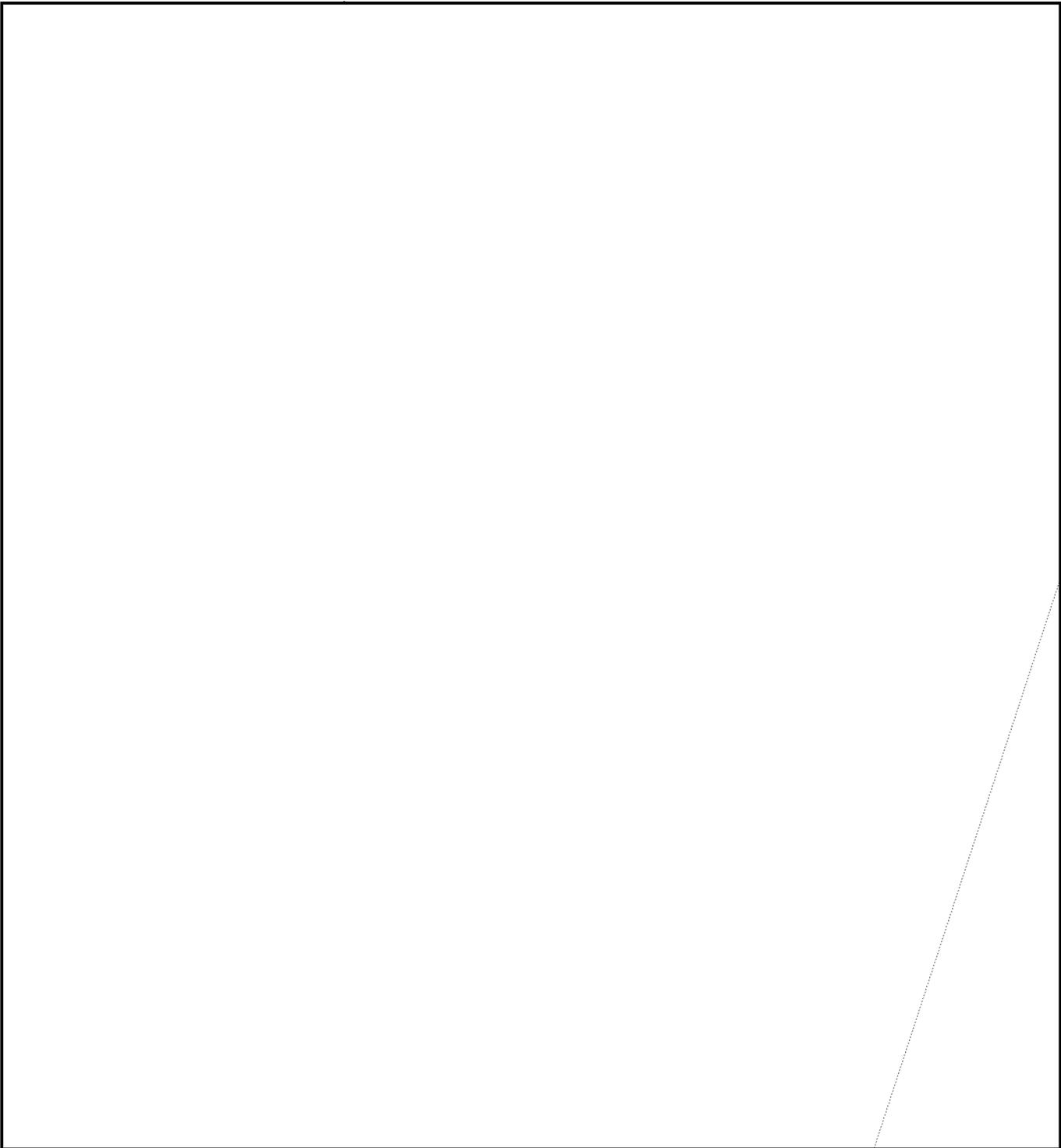
~~TOP SECRET SUNDY~~

~~TOP SECRET SUNDY - SECURITY INFORMATION~~

COPY

AFSA-23

Necessity of Plain Text in Cryptanalysis Cont'd
AFSA-23C3 28 February 1952



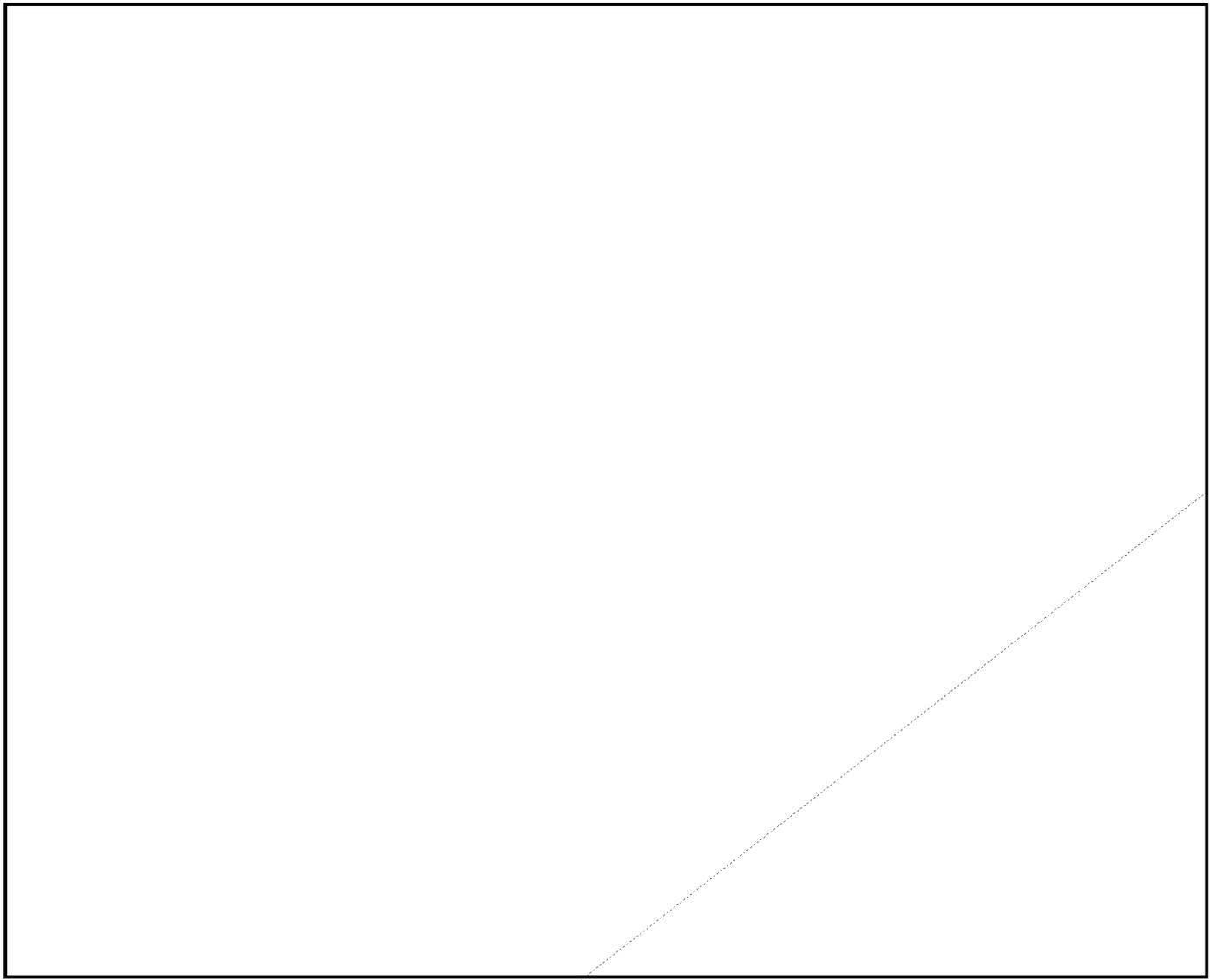
~~TOP SECRET SUNDY~~

~~TOP SECRET GUIDE - SECURITY INFORMATION~~

COPY

AFSA-23

Necessity of Plain Text in Cryptanalysis Cont'd
AFSA-23C3 28 February 1952



ELIZABETH R. BROWNELL
AFSA-23C3

EO 3.3(h)(2)
PL 86-36/50 USC 3605

~~TOP SECRET~~