DEPARTMENT OF DEFENSE
ARMED FORCES SECURITY AGENCY
WASHINGTON 25, D. C.

IN REPLY REFER TO

Serial: 00087

OGA

8 APR 1952

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

MEMORANDUM FOR [redacted]

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 ot 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.

William F. Friedman

WILLIAM F. FRIEDMAN
Consultant

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

Returned to AFSA-14 7 July 52 WFF

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. See also Public Law 513, 81 Congress second session

~~TOP SECRET~~

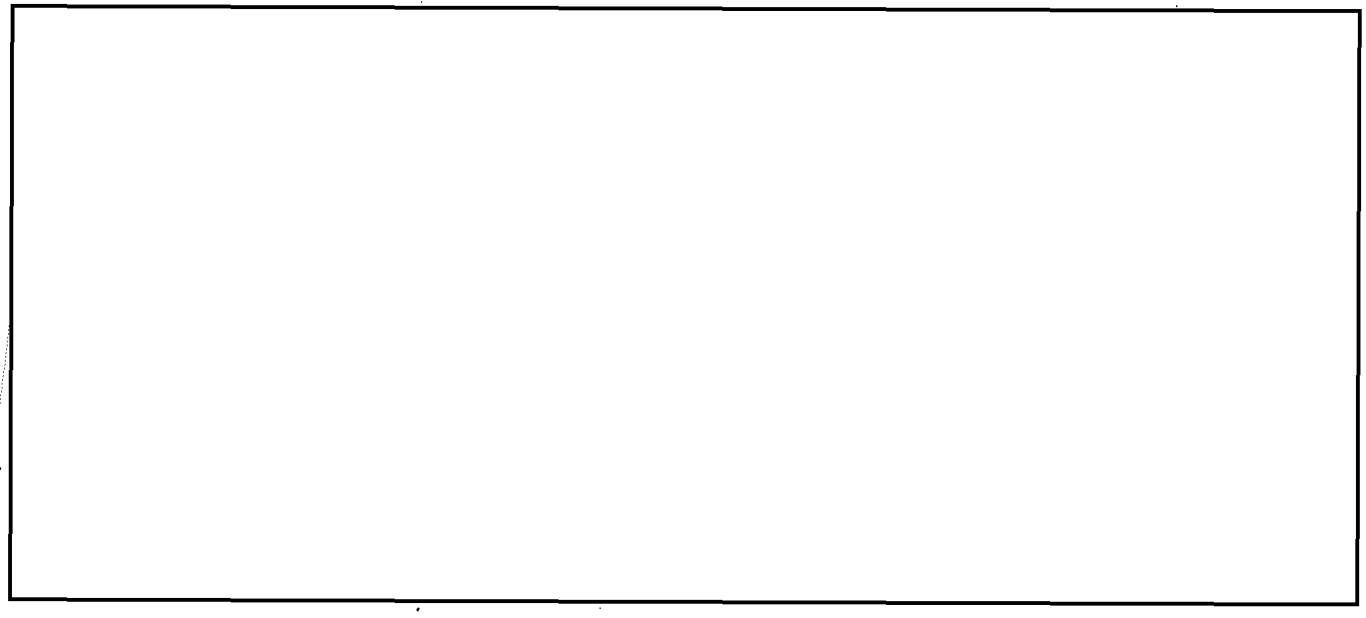
Necessity of Plain Text in Cryptanalysis

AFSA-23 AFSA-23C3 28 February 1952

1. All sections of AFSA 23C 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.

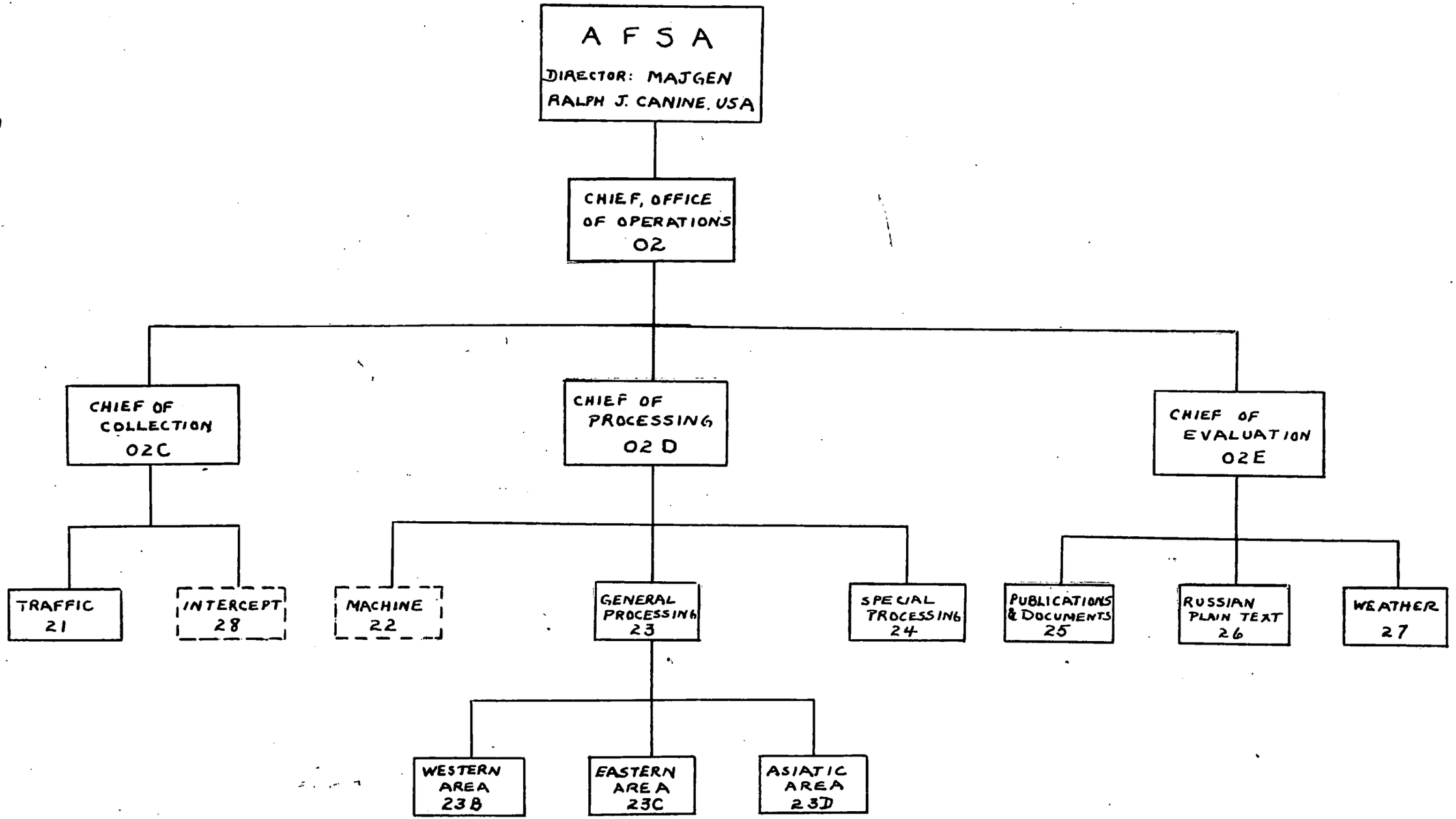
2. A cryptographic system is not solved in a vacuum nor in an ivory tower of abstract mathematics. The basis of operations at AFSA, namely that one operating unit shall process the traffic of a specific country, cipher and plain text, has proved its value. This method has involved the correlation of 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:



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

ELIZABETH R. BROWNELL
AFSA-23C3

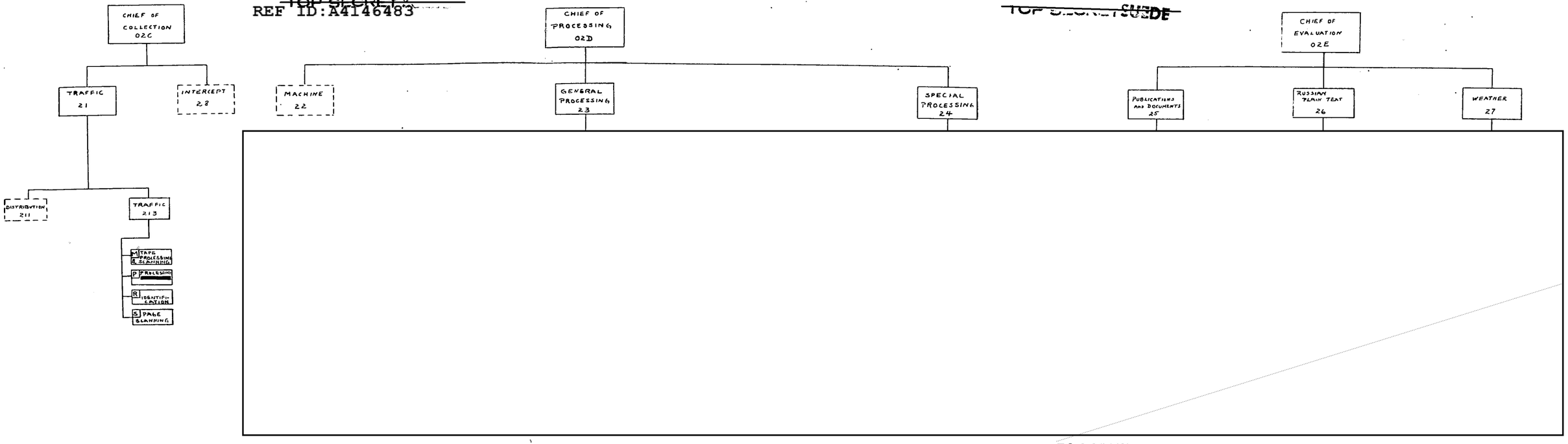


App. 2

REF ID:A4146483

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

App 3



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

App 4