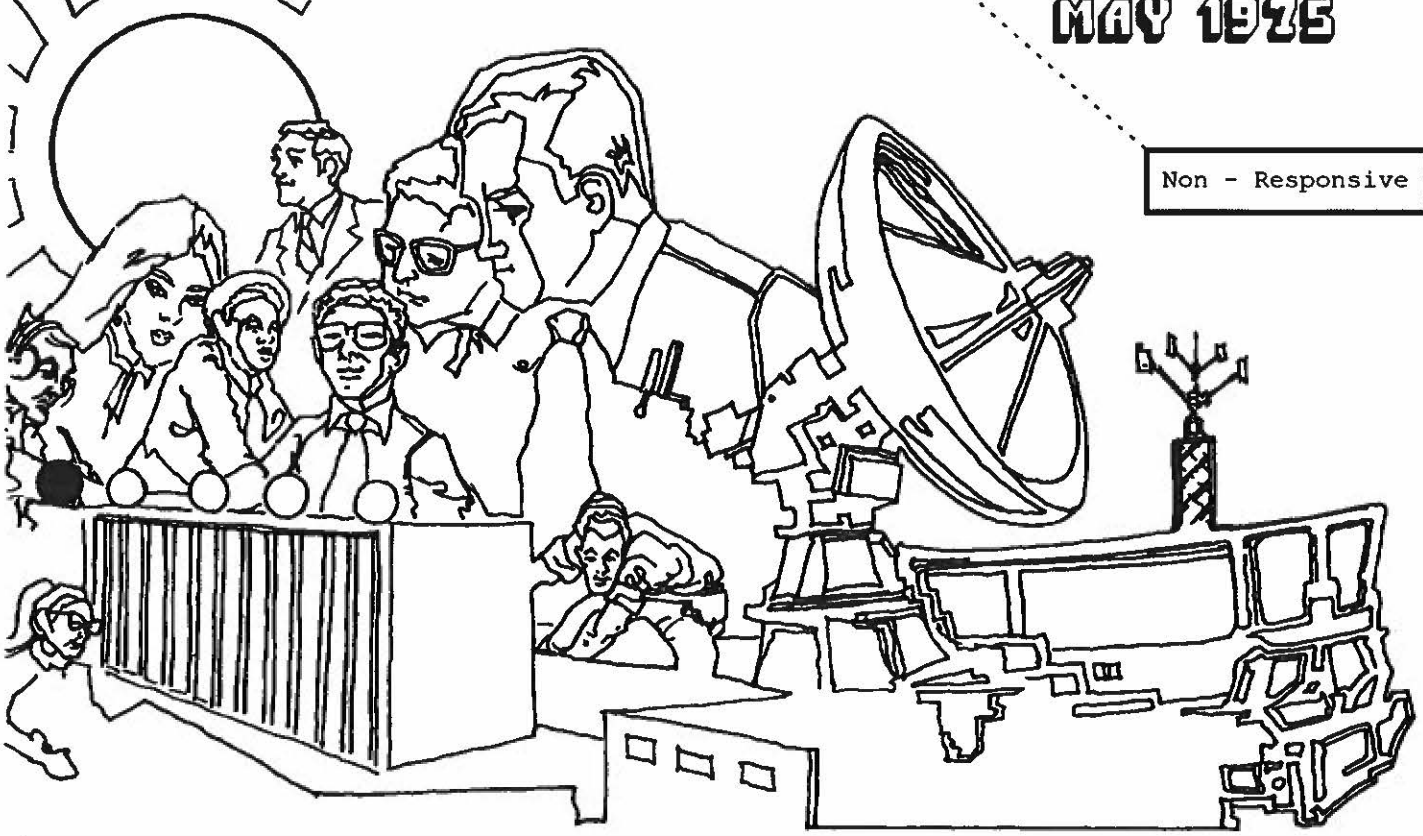
~~TOP SECRET~~ 980

NATIONAL SECURITY AGENCY
FORT GEORGE G. MEADE, MARYLAND

[redacted] TOLOG

MAY 1975



Non - Responsive

TA, HANDMAIDEN OF CA.....Frederic O. Mason.....3

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~

~~TOP SECRET~~

Classified by DIRNSA (NSAM 123 dtd [redacted])
Exempt from GDS, EO [redacted], Category 2
Declassification Notification by the Originator

Declassified and Approved for Release by NSA on 03-10-2021 pursuant to E.O. 13526, MDR Case #109386

Non - Responsive

Non - Responsive

Non - Responsive

EO 3.3b(3)
PL 86-36/50 USC 3605

TA, HANDMAIDEN OF CA

FREDERIC O. MASON, JR., P11

Traffic analysis was created, as an analytic function, in order to organize collection and to maintain continuity for support of cryptanalysis. In a broad sense it still does that, but it has also achieved a value of its own.

Before TA was fragmented into many career fields (for reasons which escape me) it was everything in COMINT which wasn't CA, or--more properly--it was a subset of CA, employing many CA techniques, but against a different body of data.

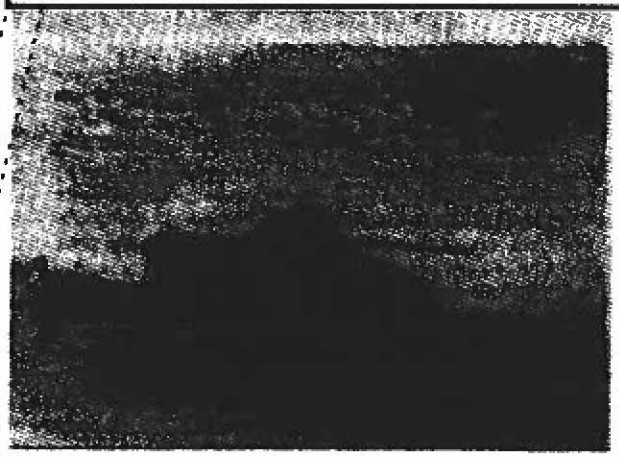
The essential differences between CA and TA are twofold:

CA works against data which is wholly logical, since the recipient of an encrypted message must know and use the same rules as the originator in order for communication to succeed, whereas TA works against data which is often (even usually) logical, but with discontinuities, changes in plan, permissible.

Generally the two skills are inversely important: if CA is very successful, TA is apt to be little valued (though very complete); if CA is stymied, then any TA achievement is valued highly.

In practice the line between the two is not sharp, since TA normally does many "trivial" cryptanalytic jobs

TA and CA are, then, both similar and interdependent.



EO 3.3b(3)
PL 86-36/50 USC 3605

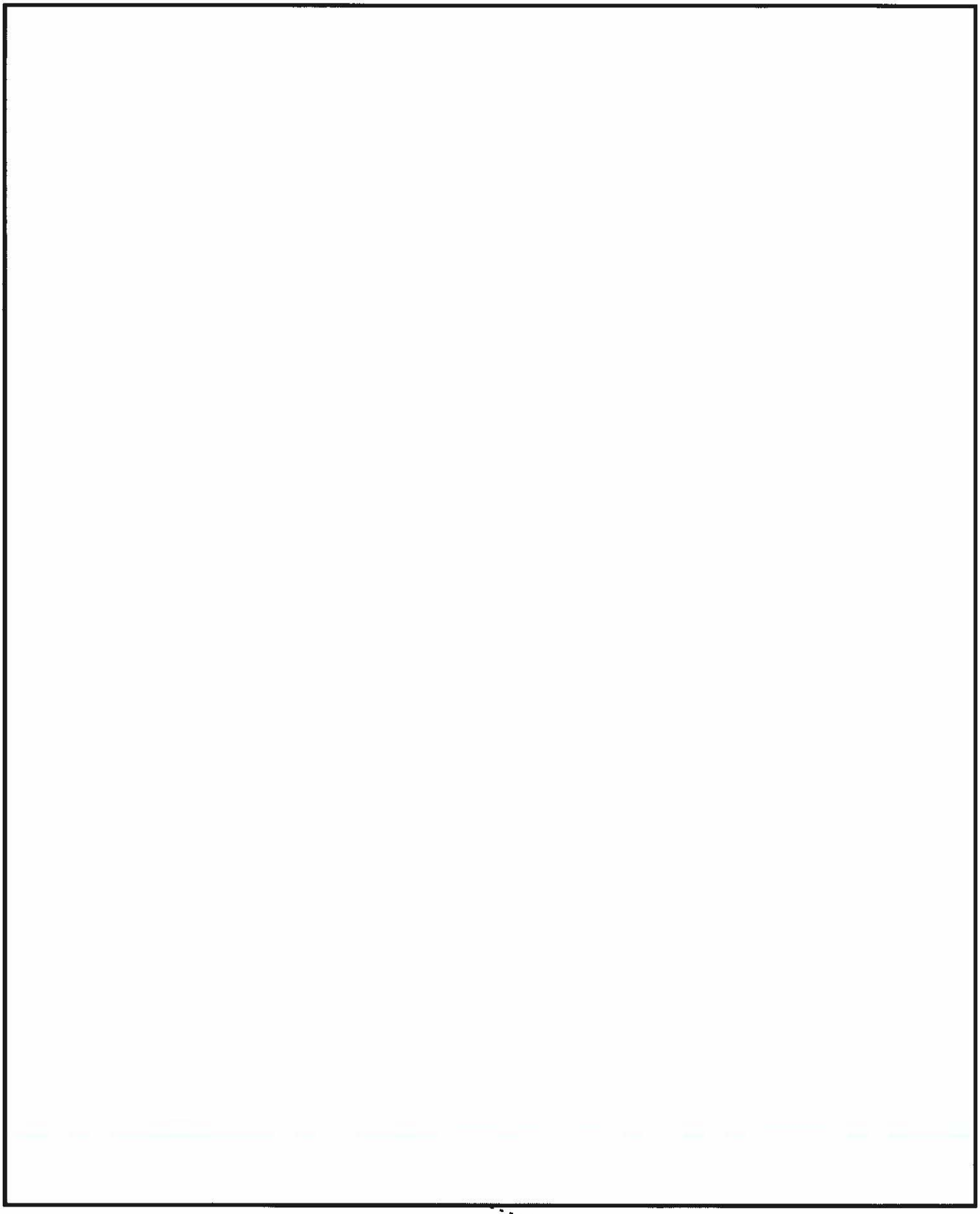
Therefore, flexing our crypto-TA muscles is, in addition to being fun for people who like puzzle-solving, useful practice against future urgent need for these skills.

Boiled down to essentials and stripped of steps which consume much TA effort), the analytic processes of TA are reasonably straightforward. However, as the following example will illustrate, a considerable amount of careful work is required, even for small problems. To appreciate the real problem, you should know

But try your hand at a small problem which can be solved in an hour or two because the

EO 3.3b(3)
PL 86-36/50 USC 3605

If this sort of exercise entertains you, we can do some more. Let us know.


Non - Responsive

Non - Responsive

~~TOP SECRET UMBRA~~

~~TOP SECRET UMBRA~~

Non - Responsive

Non - Responsive

EO 3.3b(3)
PL 86-36/50 USC 3605

Non - Responsive

ANSWERS TO CLASSIFICATION PROBLEMS

1. TOP SECRET/HANDLE VIA COMINT CHANNELS ONLY. See USSID 3 or the Classification Manual. "Information revealing the extent or nature of COMINT collaboration with specific foreign governments, including written agreements establishing such collaboration" will be classified TS-CCO. (The subject of Soviet naval communications is too broad to require a Codeword.)

2. SECRET CODEWORD. See USSID 3, Annex A, Appendix 2:

3. SECRET/HANDLE VIA COMINT CHANNELS ONLY. Authority: judgment. This abstract shows (1) our interest in collecting certain signals from (2) our intention to establish ground-based remote intercept sites to accomplish this, and (3) the association of three covernames with this subject. While point (1) by itself would require only CONFIDENTIAL/COMINT CHANNELS, the combination of (1), (2) and (3) requires a SECRET classification with COMINT Channels protection.

4. SECRET/HANDLE VIA COMINT CHANNELS ONLY. NSA Classification Manual, page 40. Any indication of COMINT liaison or collaboration between NSA and Second Parties is S-CCO. So is any

5. SECRET CODEWORD. Judgment. This item reveals the time and place of acquisition of an enciphered signal. Although the frequency is not given, it does reveal a new success. More definitive information would require TOP SECRET CODEWORD.

6. CONFIDENTIAL/COMINT CHANNELS. NSA Classification Manual, page 40. "Statements disclosing the COMINT indoctrinated or debriefed status of individuals and lists of COMINT indoctrinated and debriefed personnel" are C-CCO.

7. TOP SECRET CODEWORD. USSID 3, Annex A, Appendix 1. "All diplomatic systems, regardless of degree of cryptographic sophistication."

8. SECRET CODEWORD. The most revealing thing here is the callwords. Although we do not have a time reference, the item implies the current time. Such being the case, it would require little effort on the part of the enemy to research the use of these callwords. The fact that the identity cannot be determined as one of several possibilities points out our success in this field.

9. CONFIDENTIAL/COMINT CHANNELS. NSA Classification Manual, page 41. The mention of a target, such as only requires CONFIDENTIAL, but the caveat "HANDLE VIA COMINT CHANNELS ONLY" is, itself, classified CONFIDENTIAL/HANDLE VIA COMINT CHANNELS ONLY.

10. SECRET CODEWORD. USSID 3, Annex A, Appendix 3, paragraph 1.5. The report serial (X/00/3415-75) tells you that the original report was Subcategory II (X), or SECRET MORAY. However, the message you are being asked to rule on is a technical message and not product, and USSID 3 explains, "Technical material relating to Category II (X) product is published as Category II."

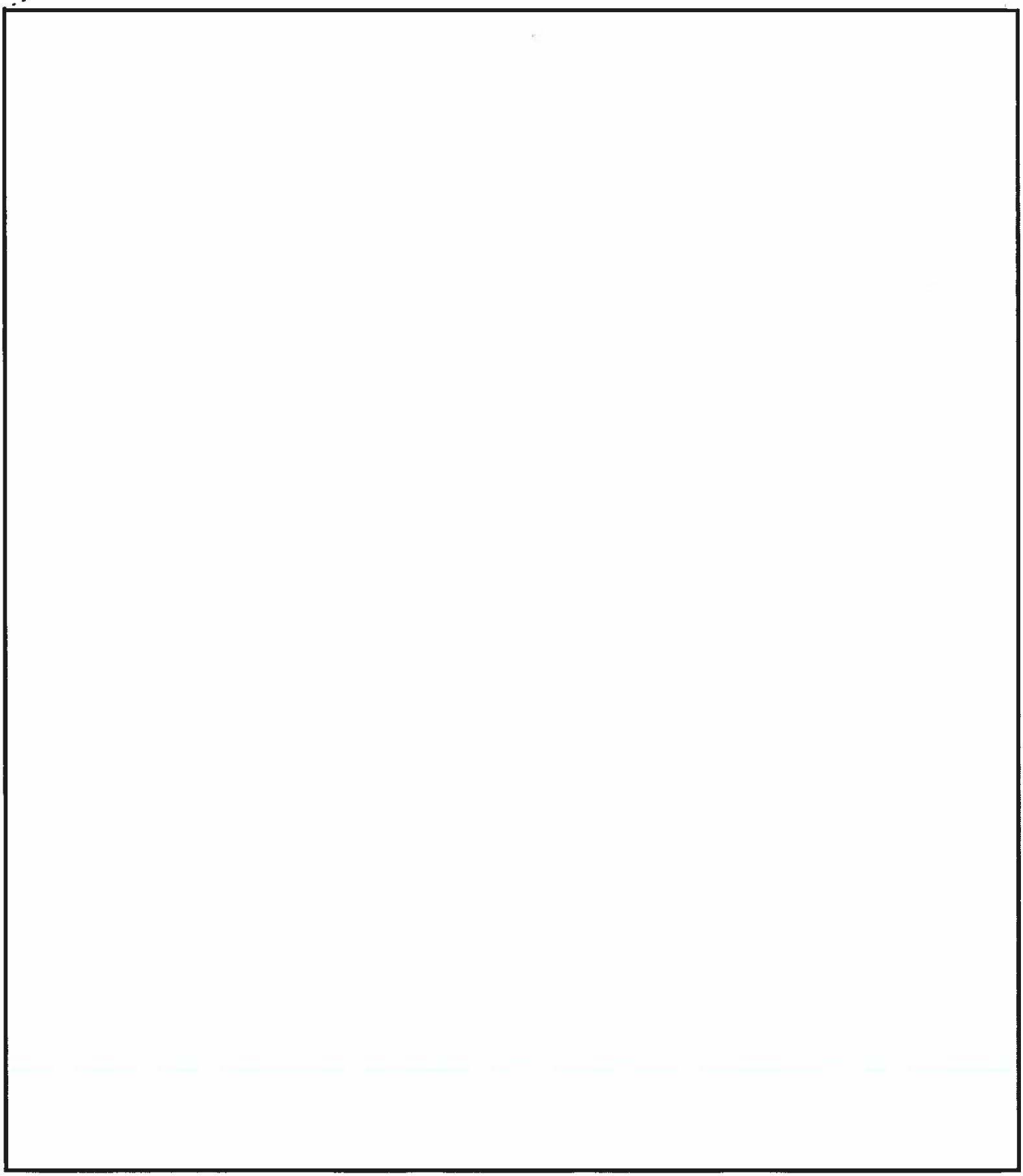
I hope this exercise clearly demonstrates the problems and difficulties involved in determining classifications, and specifically what information needs Codeword or "COMINT Channels" protection. There are eight Classification Advisory Officers at NSA. They are willing to offer assistance in your classification problems, but the responsibility for proper classification belongs to each of us. My advice then is to use the Classification Manual and USSID 3, consult your Classification Advisory Officer when necessary, and most important, take the time to determine the appropriate classification and thus to insure that the proper protection is being afforded.

(~~TOP SECRET UMBRA~~)

EO 3.3b(3)
PL 86-36/50 USC 3605

EO 3.3b(3)
EO 3.3b(6)
PL 86-36/50 USC 3605

Non - Responsive



Non - Responsive

CONFIDENTIAL

CONFIDENTIAL HANDLE VIA COMINT CHANNELS ONLY

Non - Responsive

Non - Responsive