

BEST COPY

Available

*THROUGHOUT
FOLDER'S*

6/24/98

SECRET

001563 -5378
3-6210

MEMORANDUM FOR: Executive Director

VIA: Deputy Director for Plans *LS/RK*

SUBJECT: Review of Agency Use of Cryptonyms

REFERENCE: Executive Director Memorandum of 19 November 1963

1. Reference memorandum recommends a critical look be taken at the Agency use of cryptonyms in cable traffic. The recommendation proceeds from a premise that Agency communications and physical security have tightened considerably since the last review of this subject.

2. This memorandum is a statement of the CI Staff views regarding the various points raised in reference memorandum.

3. The Director of Communications has stated in substance as follows:

a. There is no technical security requirement for the use of cryptonyms in Agency cable communications.

b. Garbled cables can be degarbled more easily if the meaning is not made unclear by the use of cryptonyms, and cryptonyms do not necessarily result in a reduction of the length of the cable; thus, the clearer the meaning of the cable, generally the shorter is the processing time.

No exception can be taken to the foregoing statements. It is observed from experience, however, that a communications

GROUP 1
Excluded from automatic
downgrading and
declassification

SECRET

SECRET

system which is secure today may not be so twenty years from today, and that the use of cryptonyms is a form of insurance against future contingencies.

4. Reference queries ' where we must use cryptonyms for security reasons and where we can eliminate cryptonyms with no sacrifice of security'. A reply is succinctly provided in

25X1A

25X1A

[Redacted]

Such use, however, is not a guarantee of security and does not obviate the need for additional security measures. Cable security does not terminate with the transmission of the message. The information contained in the document requires constant protection and the presence of codes in the document is one way of providing a measure of security.

5. Recent study and observation in the CI Staff indicates that there is not an 'overuse of cryptonyms where there is no longer a valid security reason for doing so'. We have noted, however, an occasional misuse of cryptonyms in that a cryptonym will be used and that cryptonym will be compromised in the text of the same cable, e. g.:

- a. Use of cryptonyms in the summarization of an identified newspaper article.
- b. Use of cryptonyms for Ambassadors, Prime Ministers, domestic or foreign organizations in reporting their activities, when the activity has been publicized or serves in and of itself to identify the performer.

Correction of such errors is a matter of training and discipline for individuals, rather than the abandonment of the security obtained through the use of cryptonyms.

6. As to the slow-down in the administrative process occasioned by the use of cryptonyms in cables, it has been determined that Area Division Officers, and CS Staff Officers,

SECRET

SECRET

who take and coordinate action on operational cables, are knowledgeable of the meaning of each cryptonym. The Cable Secretariat 'breaks out' the cryptonyms for the DCI, DDCI, EDCI, IG, DD/P, and ADD/P. Beyond that point it is believed that the security of the message, even within the Headquarters building, takes precedence over the necessity for priority collateral administrative processing. In exceptional situations the 'break out' by Cable Secretariat can be extended.

7. Operations officers in the field stations are fully knowledgeable of the meaning of the cryptonyms with which they deal. Though physical security may 'have tightened considerably since the last review', it was established in a security seminar, which took place in Headquarters in November 1963, that physical security in the field is considerably less than desirable for a variety of reasons. The complexities of security in the field require constant review. Classified documents maintained in field stations must have the protection obtained through the use of cryptonyms. The matter of building facilities, local hires, char people, and penetrable safe equipment, is a continuing problem.

8. Possibly the most significant factor to be considered in the examination of this issue is that the Clandestine services Records Committee in 1963 took action to incorporate cable traffic into the WALNUT system in the field, in order to reduce the volume of records maintained in the field and to provide for easy destruction in the event of emergency. Cables are micro-filmed and placed on aperture cards at Headquarters and pouched to the field. Pouch security procedures require the sterilization of the material contained on the aperture cards. Thus, any consideration of a reduction in the use of cryptonyms becomes moot in terms of controlling decisions already reached.

9. If we assume for the moment, for the sake of discussion, that there is in fact an excessive use of cryptonyms, pseudonyms, and identity cables, we are immediately confronted with the point of how to correct the situation. Accepting the premise that we will not discontinue the use of code designations, the question of what constitutes 'excessive use' becomes a matter

SECRET

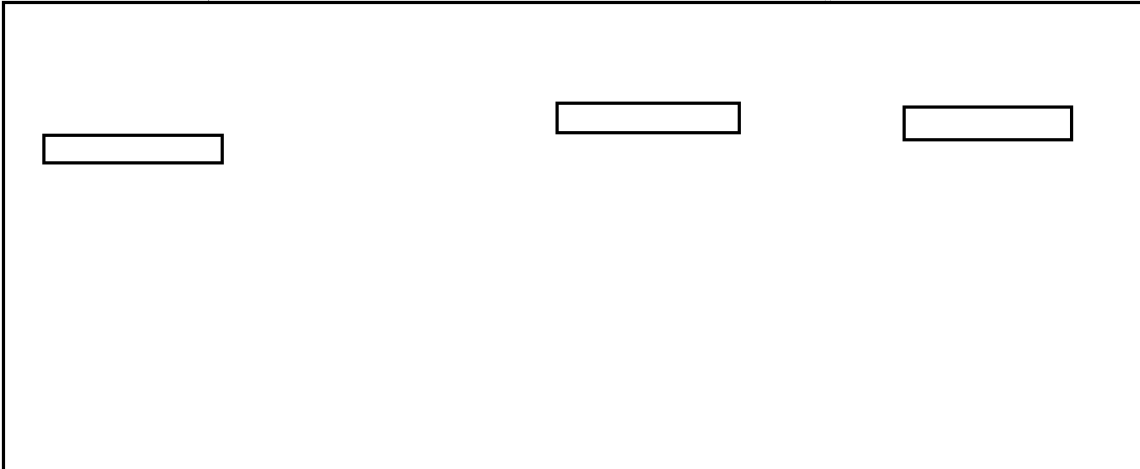
SECRET

of interpretation in each individual cable. Correction can come about only through the creation of an awareness of the problem on the part of those employees preparing and releasing cables. Such action was taken in 1957 through the issuance of [redacted] We would concur in the re-issuance of a similar notice at the present time.

25X1A

25X1

25X1A
25X1A



25X1

believe that a general review of this alleged problem could result in any material improvement.

11. As to the compromise of cryptonyms, it has been determined that compromised cryptonyms relating to agents and operations are promptly replaced by operational components. The possible exception exists in the case of cryptonyms relating to the Agency and certain of its components, and to other U. S. and foreign government agencies. For example, by strict interpretation it can be accepted that KUBARK, ODACID, and several others readily in mind, have been compromised in many ways over a period of years. They are in such constant use, however, that if they were changed, the new cryptonym would become similarly polluted in a very short time. Why then continue the use of such cryptonyms? Only because their

25X1A



12. In conclusion the CI Staff recommends that this general issue is not one calling for specific correction in the

SECRET

absence of reference to specific instances of excessive application
of the principles of good security.

James Angleton
Chief, Counter Intelligence Staff

cc: Director of Communications) via DD/S
Director of Security)

UNCLASSIFIED CONFIDENTIAL SECRET

25X1A

CENTRAL INTELLIGENCE AGENCY
OFFICIAL ROUTING SLIP

| TO | NAME AND ADDRESS | DATE | INITIALS |
|----|-------------------|---------|----------|
| 1 | D D/sec | 13 Jan. | HJO |
| 2 | D L/sec | 13 Jan | HSS |
| 3 | [Redacted] | | |
| 4 | | | |
| 5 | | | |
| 6 | Janet (this file) | | |

(I briefed on this matter by info & file per [initials])

| | | |
|--------------------------|--------------------------|--------------------------|
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

[Redacted] states he can tell you in on any aspects of the attached report from [Redacted]

25X1A

FOLD HERE TO RETURN TO SENDER

FROM: NAME, ADDRESS AND PHONE NO. DATE

[Signature] 1/13

UNCLASSIFIED

INTERNAL USE ONLY

CONFIDENTIAL

SECRET

Approved for Release 2002/05/02 : CIA-RDP83B00823R000100010001-5

ROUTING AND RECORD SHEET

SUBJECT: (Optional)

FROM:

Chief, CI Staff

EXTENSION

NO.

DATE

12 Dec 1963

TO: (Officer designation, room number, and building)

DATE

OFFICER'S INITIALS

COMMENTS (Number each comment to show from whom to whom. Draw a line across column after each comment.)

RECEIVED

FORWARDED

1.

DD/S

13 Dec 63

17 Dec 63

VT

2.

3.

Director of Security

4.

5.

6.

7.

8.

9.

10.

11.

12.

13.

14.

15.

Bob,

Col White would be interested in oral briefing on this when you have read it.

V.T.

Read with interest



10 JAN 1964

25

STANDARD FORM NO. 64

File
Office Memorandum • UNITED STATES GOVERNMENT

25X1A TO :

[Redacted]

FROM :

you info HK
Comu + Q said OK

SUBJECT:

25X1A

[Redacted]

on [Redacted] I open
attached (D.L. 15 Dec), but
asked if some change can
be agreed. [Signature]

cc-1996

Chief, Counter Intelligence Staff

29 NOV 1965

Director of Communications

Review of Agency Use of Cryptonyms

REF : Action Memorandum No. 315

1. Having reviewed the reference, I wish to make two comments from the standpoint of the Office of Communications:

a. Since CIA cable communications are enciphered in category A cryptographic systems, there exists no technical communication security requirement for the use of cryptonyms in CIA cable communications.

b. It is a fact that the clearer the meaning of a cable, generally the shorter is the processing time. The reason for this is twofold. First, cables which are mutilated in transmission are more easily and quickly degarbled when the clear meaning of the text is apparent. Second, the apparent reduction in cable length which the use of cryptonyms affords is often negated by the requirement to repeat seldom used or unusual words.

2. Recognizing that there are many other factors which bear on the decision to employ cryptonyms in CIA cable communications, I am forwarding the foregoing for consideration in your review of the subject.

[Redacted]

25

GROUP 1
Excluded from automatic
downgrading and
declassification

SENDER WILL CHECK CLASSIFICATION TOP AND BOTTOM

UNCLASSIFIED CONFIDENTIAL SECRET

CENTRAL INTELLIGENCE AGENCY
OFFICIAL ROUTING SLIP

| TO | NAME AND ADDRESS | DATE | INITIALS |
|----|-----------------------|----------|----------|
| 1 | DD/S | 11-21-63 | W |
| 2 | D/Security - GE 31 Hq | 22 Nov | RSB |
| 3 | DD/Sec | 22/11 | Hjo |
| 4 | DD/PPS * | | |
| 5 | | | |
| 6 | | | |

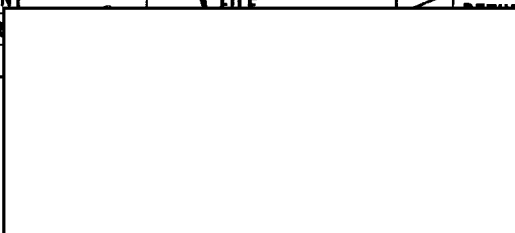
| | | | | | |
|--------------------------|----------|-------------------------------------|--------------|--------------------------|----------------|
| <input type="checkbox"/> | ACTION | <input type="checkbox"/> | DIRECT REPLY | <input type="checkbox"/> | PREPARE REPLY |
| <input type="checkbox"/> | APPROVAL | <input checked="" type="checkbox"/> | DISPATCH | <input type="checkbox"/> | RECOMMENDATION |
| <input type="checkbox"/> | COMMENT | <input type="checkbox"/> | FILE | <input type="checkbox"/> | RETURN |
| <input type="checkbox"/> | CONCUR | <input type="checkbox"/> | | <input type="checkbox"/> | SIGNATURE |

25X1A

Remarks:

1 to 2

Bob:



Handwritten signature

CI Staff has action here.. I assume they will coordinate with you. I will be interested in being briefed orally and informally on the outcome.

* No 4 for action - LKW
Pls note deadline 2 Dec 63

FOLD HERE TO RETURN TO SENDER

| | |
|-----------------------------------|------|
| FROM: NAME, ADDRESS AND PHONE NO. | DATE |
| | |

SECRET

(CLASSIFICATION)

DD/S 63-4952

Executive Registry
63-8668

OFFICE OF THE DIRECTOR

Action Memorandum No. 315

Date 19 November 1963

**A
C
T
I
O
N

M
E
M
O
R
A
N
D
U
M**

TO : Chief, Counter Intelligence Staff

VIA : Deputy Director/Plans

SUBJECT : Review of Agency Use of Cryptonyms

REFERENCE:

1. I believe the time is appropriate to take a new look at certain aspects of our use of cryptonyms in cable traffic. Our communications and physical security have tightened considerably since the last review. These points, in particular, should be considered:

a. Do we overuse cryptonyms where there is no longer a valid security reason for doing so? Even though the use of cryptonyms sometimes simplifies the drafting of cables for officers familiar with a fixed set of cryptonyms, they generally make their reading much slower, especially by senior officers who cannot be familiar with all the cryptonyms. I would like to know where we must use cryptonyms for security reasons and where we can eliminate cryptonyms with no sacrifice of security. I recognize there will be certain grey areas.

b. It is my understanding that a great many cryptonyms now in use have been compromised at least once and should be changed or dropped.

25X1A

25X1A



SUSPENSE DATE:

SECRET

GROUP 1
Excluded from automatic
downgrading and
declassification

(CLASSIFICATION)

SECRET

d. We should also consider the fact that Agency cables with cryptonyms go to Agency components where they are handled by personnel who are not disciplined in cryptonym procedure.

2. Please let me have by 2 December your recommendations for reviewing our cryptonym procedure; I would like your opinion on what specific corrections and changes should be made before any actual work is begun.

(signed) Lyman B. Kirkpatrick

Lyman B. Kirkpatrick
Executive Director

cc: Director of Communications ()
✓ Director of Security () via DD/S

NOV 5 1983

NOV 5 1983

Office Memorandum • UNITED STATES GOVERNMENT

TO :

DATE:

25X1A

FROM :

SUBJECT:



Review of agency use of Cryptology.
 Part 7 ~~...~~ "Though the actual
~~...~~ " ~~...~~ ^{Shield adds} ~~...~~ 1/3" that
 physical security in the " - - -
 suggest at read that the completion
 of physical security in the field
~~...~~ ~~...~~ ~~...~~ ~~...~~
 review

OPTIONAL FORM NO. 10

UNITED STATES GOVERNMENT

SECRET

Memorandum

DATE: 9 December 1963

TO :

FROM :

25X1A

SUBJECT: Review of Agency Use of Cryptonyms

25X1A

Para 7, line 13 reads "that physical security in the"
-- suggest it read that the complexities of physical security
in the field requires constant and continuous review.

*talked to
12/9/63 3PM
he said the
no insert*

GROUP 1
Excluded from automatic
downgrading and
declassification

BEST COPY

AVAILABLE

~~SECRET~~

MEMORANDUM FOR THE RECORD:

SUBJECT: Memorandum from Executive Director dated 19 November 1963/Review of Agency Use of Cryptonyms

1. Reference memorandum recommends a critical look be taken at the Agency use of cryptonyms in cable traffic. The recommendation proceeds from a premise that Agency communications and physical security have tightened considerably since the last review of this subject.
2. This memorandum is a statement of the CI Staff position regarding the various points raised in reference memorandum.
3. The Director of Communications has stated in substance as follows:
 - a. There is no technical security requirement for the use of cryptonyms in Agency cable communications.
 - b. Garbled cables can be degarbled more easily if the meaning is not made unclear by the use of cryptonyms, and, cryptonyms do not necessarily result in a reduction of the length of the cable; thus, the clearer the meaning of the cable, generally the shorter is the processing time.

No exception can be taken to the foregoing statements. It is observed from which experience, however, that a communications system which is secure today may not be so ~~so~~ twenty years from today, and that the use of cryptonyms is a form of insurance against future contingencies.

25X1A

4. Reference queries "where we must use cryptonyms for security reasons and 25X1A where we can eliminate cryptonyms with no sacrifice of security". A reply is succinctly provided in [redacted] wherein it is stated that [redacted]

25X1A

[redacted] relationship to CIA. Such use, however, is not a guarantee of security and does not obviate the need for additional security measures. Cable security does not terminate with the transmission of the message. The [redacted] information contained in the document requires constant security, and the presence of codes in the document is one way of providing a measure of security.

5. Recent study and observation in the CI Staff indicates that there is not an overuse of cryptonyms where there is no longer a valid reason to do so. We have noted, however, an occasional misuse of cryptonyms [redacted] in that a ~~no~~ cryptonym will be used and that cryptonym will be compromised in the text of the same cable, e.g.:

Use of cryptonyms in the summarization of the [redacted] newspaper article.

25X1A

[redacted]

Correction of such errors is a matter of training and discipline for individuals, rather than the abandonment of the security obtained through the use of cryptonyms.

~~SECRET~~

SECRET

6. As to the slow-down in the administrative process occasioned by the use of cryptonyms in cables, it has been determined that Area Division Officers, and CS Staff Officers, who take and coordinate action on operational cables, are quite ~~not~~ knowledgeable of the meaning of each cryptonym. The Cable Secretariat "breaks out" the cryptonyms for the DCI, DDCI, ~~not~~ EDCI, IS, DD/P, and AED/P. Beyond that point the CI Staff feels that the security of the message, even within the Headquarters building, takes precedence over the necessity for priority ~~processing~~ collateral administrative processing. In *exceptional* situations the "break-out" by Cable Secretariat would appear to be adequate. Operations officers in the field stations are fully knowledgeable of the meaning of the cryptonyms with which they deal. Though physical security may "have tightened considerably since the last review", it was established in a security seminar, which took place in Headquarters in November 1963, that physical security in the field is considerably less than adequate for a variety of reasons too complex to explore in this memorandum. ~~not~~ Classified documents maintained in field stations must have the protection obtained through the use of cryptonyms. ^{and other special files} The matter of local hires, char people, and penetrable safe equipment, are a continuing problem.
7. Possibly the most significant factor to be considered in the examination of this issue is that the Central Records Committee ~~not~~ in 1963 took action to incorporate cable traffic into the WALNUT system in the field, in order to reduce the volume of records maintained in the field and to provide for easy destruction in the event of emergency. Cables are ~~not~~ microfilmed and placed on aperture cards at Headquarters and pouched to the field. Pouch/procedures require the sterilization of the material contained on the aperture cards. Thus any consideration of a reduction in the use of cryptonyms becomes moot in terms of controlling decisions already reached.

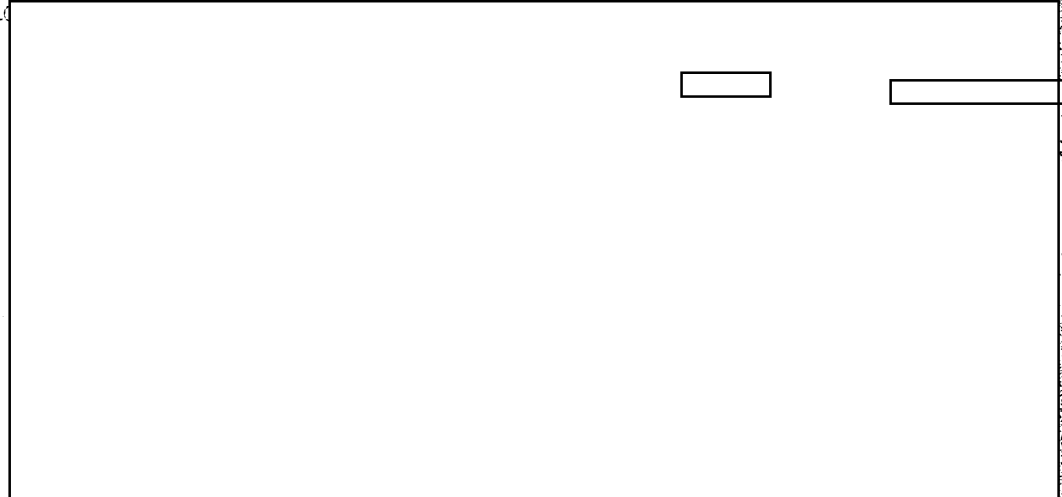
SECRET

9. If we assume for the moment, for the sake of discussion, that there is in fact an excessive use of cryptonyms, pseudonyms, and identity cables, we are immediately confronted with the point of how to correct the situation. Accepting the premise that we will not discontinue the use of code designations, the question of what constitutes "excessive use" becomes a matter of interpretation in each individual cable. Correction can come about only through the creation of an awareness of the problem on the part of those employees preparing cables. Such action was taken in 1957 through the issuance of [redacted] ^{of Releasing} Possibly the re-issuance of a similar notice is in order at the present time.

25X1A

25X1A

25X1A



25X1A

10. As to the compromise of cryptonyms, it has been determined that compromised cryptonyms are promptly replaced by operational components. The possible exception exists in the case of cryptonyms relating to the Agency and ~~SECRET~~ certain of its components, and to other ~~SECRET~~ U.S. and foreign government agencies. For example, by strict interpretation it can be accepted that KUBARK, ODACID, and several others readily in mind, have been compromised in many ways over a period of years. They are in such constant use, however, that if they were changed, the new cryptonym would become similarly polluted in a very short time. Why then continue the use of such cryptonyms? Only because their use in the

25X1A



SECRET

12. In conclusion the CI Staff recommends that this general issue is not one calling for specific correction in the absence of specific reference to instances of excessive application of the principles of good security.

[Redacted]
CI Staff

25X1A

SECRET