~~SECRET~~ Serial:

MEMORANDUM FOR EXECUTIVE SECRETARY USCIB AND USCSB

SUBJECT: Provision of Communications Security Assistance to Foreign Governments.

It is requested that the attached be distributed to the members of both boards for consideration at the forthcoming joint meeting.

This was never sent — A greatly modified paper replaced it.

~~SECRET~~

MEMORANDUM FOR MEMBERS, UNITED STATES COMMUNICATIONS INTELLIGENCE BOARD AND MEMBERS, UNITED STATES COMMUNICATIONS SECURITY BOARD

SUBJECT: Provision of Communications Security Assistance to Foreign Governments

1. The National Security Council Directive on Communications Security (NSC 168, 20 October 1953) states, in paragraph 1 c (2)(e), that it is the responsibility of the United States Communications Security Board to establish broad policies necessary to "guide the relations of the U. S. Government with foreign governments and international organizations in COMSEC matters." Among the necessary policies is one which will establish the direction under which communications security assistance can be provided to foreign nations. I have prepared a proposed USCSB directive to this end and I recommend its approval by both boards. The proposed directive is attached as Appendix A. Supplied with it for the convenience of the members is a glossary containing brief descriptions of the equipments and cryptosystems mentioned in the directive.

2. Under existing national policy, it is necessary that the State-Defense Military Information Control Committee (S-DMICC) also approve the directive. Therefore, I recommend that, after approval by USCSB and USCIB, the Executive Secretary, USCSB, forward the directive to S-DMICC for its consideration. In so doing the Executive Secretary should point out to S-DMICC that, except as otherwise indicated in inclosure 1 to the directive, the equipments listed have already been approved for release and that approval of the directive by S-DMICC will constitute approval of the releasability of the remaining items.

3. Attached as Appendix B for consideration by the members of the Boards, is a statement of my opinion of the implications of

the proposed directive.

4. With regard to USCIB 29.2/1, dated 3 May 1954, Subject: Release of AFSAM 7 for NATO National Use (circulated also as USCSB 3-1/1) the action recommended is consistent with the proposed directive. Therefore, subject to approval of the latter, I recommend favorable consideration of USCIB 29.2/1 (USCSB 3-1/1).

RALPH J. CANINE
Lieutenant General, US Army
Director

~~SECRET~~ DRAFT

US COMMUNICATIONS SECURITY BOARD DIRECTIVE #___

PROVISION OF US COMMUNICATIONS SECURITY INFORMATION AND CRYPTOGRAPHIC MATERIAL TO FRIENDLY FOREIGN GOVERNMENTS AND INTERNATIONAL ORGANIZATIONS

1. PURPOSE - The purpose of this directive is to establish USCSB policy governing the provision of United States communications security information and cryptographic material to friendly foreign governments and international military organizations, subject to approval of disclosure by appropriate US authority.

2. GENERAL POLICY -

a. The use of insecure cryptographic systems and communication practices by nations and international military organizations friendly to the US can be detrimental to the national security of the US. It shall be the general policy of the USCSB to improve the security of communications of friendly foreign nations with which the US has formal agreement for mutual defense. This may include, (1) the security of communications between US and foreign military organizations, (2) the security of communications within international military organizations with which or in which the US participates by formal agreement, and (3) the security of national communications within the foreign governments where insecurity would affect US national interests.

b. The Director, National Security Agency, is designated as Executive Agent of USCSB to carry out this policy. In this capacity, he is authorized to take such steps as he considers necessary, within policy established by the USCSB, to provide releasable cryptomaterial as described in the inclosure or assistance in communications security matters to friendly foreign governments and international military organizations.

APPENDIX A

SECRET

c. Disclosure of other specific items of cryptographic material or information not authorized in this Directive will be as approved by S-DMICC (State-Defense Military Information Control Committee). Conditions governing disclosure of classified military information to foreign nations are established by S-DMICC.

3. RELEASABLE CRYPTOGRAPHIC INFORMATION - Crypto-equipments and crypto-systems listed in the inclosure may be provided to the nations specified, provided disclosure has been approved by S-DMICC. Operating instructions, repair and maintenance instructions, and keying material to be used with these systems and equipments are considered to be an integral part of a crypto-system. The USCSB will, as necessary, amend the inclosure to conform to United States foreign policy with respect to the specified nations, and to particular cryptographic requirements.

4. PROCEDURE FOR OBTAINING AUTHORIZATION TO RELEASE - All requests for release of cryptographic information or material to foreign governments received or initiated by USCSB members will be submitted to the Director, National Security Agency.

a. When the particular information or material requested is releasable to the particular nation in accordance with this Directive, the Director, National Security Agency, is authorized to furnish, within his capabilities, the required material without referring the request to the USCSB.

b. When the particular information or material requested is not releasable as provided for in this Directive, and the Director, National Security Agency, considers the disclosure to be in the US national interests, he will refer the request with his recommendations to S-DMICC through USCSB and USCIB. The Director, National Security Agency, will provide information and advice as necessary to assist USCSB in reaching a decision.

Incl:
Four Groups

SECRET

SECRET

[redacted]

All cryptosystems and equipments listed in Groups 2, 3, and 4 plus the following are releasable to these nations:

CSP 889
ASAM 2-1
AFSAM 4A
AFSAM 9
AFSAM 21
AFSAM 36
AFSAM D17
AFSAM 499
AFSAX 500
AFSAX D503
AFSAY D804
AFSAY D806
AFSAY D808
AFSAZ 7315

AFSAM 44[1]
AFSAM 45[1]
AFSAM 498[1]
AFSAM D26[1]
AFSAM D31[1]
AFSAM D22[1]
AFSAM D37[1]
AFSAW 7200[1]
AFSAW D7224[1]
AFSAX D505[1]
AFSAY D801[1]
AFSAY D807[1]
AFSAY D809[1]
AFSAY D810[1]
AFSAY 816[1]
AFSAY 830[1]
AFSAZ 7301[1]
AFSAZ D7305[1]

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

[redacted]

Incl 1

[redacted]

All cryptosystems and equipments listed in Groups 3 and 4 plus the following are releasable to these nations:

AFSAM 7[1]

AFSAM 47B

AFSAM 25B/25C

One-time-tape cryptosystems

CSP 1752 (operational editions)

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

Additional releases:

ASAM 2-1 has been released [redacted]

CSP 889 has been released [redacted]

AFSAM 4A has been released [redacted]

[1] Not now released to [redacted]

GROUP 3 - SOUTH AND CENTRAL AMERICA (less Argentina & Guatemala), CEYLON, PHILIPPINES AND [redacted]

All cryptosystems listed in Group 4, plus the following cryptosystems and equipments are releasable to these nations:

M209 with OLYMPUS keying material[1]

VENUS cryptosystems[2]

CSP 1752 (training editions only)[2]

One-time pad systems[3]

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

[1] Was held by Brazil, Mexico, and Peru

[2] Authorized for release on need-to-know basis, but not now held by any except Colombia and Philippines

[3] Are now released only to [redacted]

~~SECRET~~

GROUP 4, [redacted] AND FRENCH INDO-CHINA

The following cryptosystems are releasable to these nations:

Authentication systems (pencil and paper)[1]

Map reference and numerical codes[1]

Operations codes[1]

Recognition and Identification systems[1]

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

[1]Provision of operational editions issued to US forces is restricted to those instances where inter-communication is required.

SECRET

GLOSSARY

GROUP 1

CSP 889 - An electromechanical, keyboard-operated, tape-printing cipher machine used for off-line literal encipherment.

ASAM 2-1 - An electromechanical cipher machine utilizing five rotors and employing principles of a code signal additive system.

AFSAM 4A - An electrically operated, 8 rotor cipher machine employing TTY principles (modified SIGMIN). May be used for off-line literal encipherment.

AFSAM 9 - A non-synchronous teletype security equipment, adaptable for synchronous use.

AFSAM 21 - A hand operated, tape printing cipher machine used in conjunction with one-time tape.

AFSAM 36 - A low echelon, hand operated, tape printing, portable cipher machine, equipped with keyboard.

AFSAM D17 - A low echelon, hand operated, tape printing, portable, pneumatic cipher machine, equipped with keyboard.

AFSAM 499 - A mechanical authentication device.

AFSAX 500 - Control console for AFSAJ 700 key generator designed for encryption of facsimile, multiplex, or single-side band teletypewriter transmissions

AFSAX D503 - A facsimile security equipment designed for the encryption and transmission of black and white copy over land-line VHF radio links.

AFSAY D804 - Single channel, self-synchronous, push-to-talk speech security equipment (ciphony).

AFSAY D806 - Single channel full duplex speech security system for use over land-line or long distance HF radio. Alternatively it can provide five teletype channels or one facsimile channel.

AFSAY D808 - Airborne ciphony equipment.

AFSAZ 7315 - Synchronous, single channel, on-line teleprinter equipment. Provides traffic flow security and automatic message numbering.

AFSAM 44 - A one-time tape teletype security equipment (on-line mixer) designed to transmit on-line and receive off-line.

AFSAM 45 - A one-time tape teletype security equipment (on-line mixer) designed for use with a printer or transmitter distributor.

~~SECRET~~

AFSAM 498 - Pneumatic authentication device.

AFSAM D26 - Single channel synchronous equipment; provides traffic flow security.

AFSAM D31 - A manually operated, tape printing, cipher device using a five level one-time key tape, intended for use as a cipher device to encrypt digital weather information.

AFSAM D22 - Electronic key generator designed for use with the AN/FGC Electronic Multiplex Equipment.

AFSAM D37 - A broadcast teletype security equipment which will include a crypto-component and synchronizing and transmission circuitry necessary to secure the output of any standard teletype device.

AFSAW 7200 - Equipment consists of random key generator, associated electronic circuits and five tape punches. (One-time tape production equipment.)

AFSAW D7224 - Equipment consists of a random key generator and associated electronic circuits, a set of 5 punches and tape checking means.

AFSAX D505 - A facsimile security equipment designed for the encryption and transmission of black and white copy over long distance wire lines or HF radio.

AFSAY D801 - Single channel self-synchronous push-to-talk speech security equipment for use as an intercommunication system over short wire links of excellent frequency response.

AFSAY D807 - Forty-eight channel, full duplex, microwave radio relay speech security equipment.

AFSAY D809 - Single channel push-to-talk speech security system for general use over wire lines.

AFSAY D810 - Single channel low echelon speech security system.

AFSAY 816 - Eight channel full duplex microwave radio relay speech security equipment.

AFSAY 830 - Single channel, push-to-talk airborne speech privacy equipment.

AFSAZ 7301 - Light weight, electromechanical tape reader for encipherment and decipherment for use with various cipher machines.

AFSAZ D7305 - A short term message synchronizer for use with the AFSAM 9 and similar teletype security equipments.

~~SECRET~~

GROUP 2

AFSAM 7 - A keyboard-operated, tape-printing cipher machine which encrypts literal text and numerals.

AFSAM 47B - A keyboard-operated, tape-printing cipher machine which encrypts literal text and numerals. Cryptographically identical with AFSAM 7.

AFSAM 25B/25C -An electromechanical, keyboard-operated, tape-printing cipher machine used for off-line literal encipherment.

CSP 1752 - Radio call sign cipher (Keylist for CSP 1750).

GROUP 3

M 209 - Hand operated, tape printing, portable mechanical cipher machine.

VENUS - A cryptosystem which provides polyalphabetic substitution with mixed unrelated alphabet strips.

One-time tape - Non-repeating key supplied in tape form.

One-time pad - Non-repeating key supplied in pad form.