

~~COPI~~Declassified and approved for release by NSA
on 09-19-2013 pursuant to E.O. 13526

Serial: 00427

24 June 1952

~~SECRET~~~~SECRET SECURITY INFORMATION~~

Captain Lee W. Parke
Chief, Division of Cryptography
Department of State
Washington 25, D. C.

Dear Captain Parke:

I have no objection to State Department use of the particular embodiment of the electrical stepping principle described in your letter of 16 June.

A security study of the proposed machine has been initiated in this Agency. Upon completion of this study you will be informed of the results.

Certain minimum physical security standards as previously discussed, which are similar to those required by the Armed Forces for their high-level cipher machines, will have to be provided.

Sincerely,

/s/Ralph J. Canine

RALPH J. CANINE

Major General, US Army

Director, Armed Forces Security Agency

cc: AG (3)

04 Comeback (1)

04 Mailroom (1)

04 Daily File (1)

412 Day File (1)

R.H.Shaw/412/372/mt/19 Jun 52

Col.R.S.Sears/04/501/vrs/20 Jun 52

HRPeterson/AG/60219/hsh/20 Jun 52

MEMO FOR RECORD:

The State Dept. is now using a cipher machine which is essentially the cryptographic equivalent of AJAX and HERMES. All attacks which work on AJAX and HERMES work on the CSP 2200. It is considered imperative that the State Dept. proceed at once to improve their cryptographic position.

The machine which is described in Captain Parke's letter is a modification of the ECM/SIGABA in which the stepping of the control maze has been changed to correspond to that in the CSP 2900, and in which the index maze has been removed and replaced with the Jones Plug.

Compromise by overrunning an embassy would compromise the principle of electrical stepping, but would not compromise the embodiment of it found either in the ECM/SIGABA or in the CSP 2900.

~~SECRET~~