

SECURITY CLASSIFICATION (If any)

DISPOSITION FORM~~SECRET~~~~CONFIDENTIAL~~*J*

FILE NO	SUBJECT		
	The National Communications Security Materiel Program		
TO	FROM	DATE	COMMENT NO 1
Distribution	DD/COMSEC	Capt. WBJakeway/60546/1u	

1. Forwarded herewith for your information and retention is the National Communications Security Materiel Program which was prepared by this Office for submission by the Director, NSA, to the United States COMSEC Board (USCSB). The program was approved by the Board on 5 November 1954.

2. Copies of a previous version of the program entitled "The National Mid-Range COMSEC Program," dated March 1954 and forwarded under cover of D/F dated 12 April 1954, and any other versions dated prior to September 1954 should be destroyed.

3. This correspondence may be downgraded to ~~CONFIDENTIAL~~ upon removal of the inclosure(s).

F. E. Herrelko
F. E. HERRELKO
Colonel, USAF
Deputy Director,
Communications Security

Incl:
a/s

Distribution:

DIR (# 26)
V/DIR (# 27)
C/S (# 28)
DC/S (# 29)
S/ASST (Mr. Friedman) (# 30)
S/ASST (Capt. Holtwick) (# 31)
P/P (2) (# 32, # 33)
COMP (2) (# 34, # 35)
LOG (2) (# 36, # 37)
R/D (2) (# 38, # 39)
T&C (# 40)
CQI (# 41)
41 (# 42)
42 (# 43)
43 (# 44)
403 (# 45)
402 (# 46, # 47)
(# 48 through # 80 held in 402)
COMSEC (2) (less incl)

Declassified and approved for release by NSA on 01-30-2014 pursuant to E.O. 13526

~~SECRET~~

30

**THE
NATIONAL
COMMUNICATIONS SECURITY
MATÉRIEL PROGRAM**

**PART I - Current Equipments and Mid - Range
Development**

PART II - Current Cryptomaterial Production

~~SPECIAL HANDLING REQUIRED~~

~~NOT RELIABLE TO FOREIGN NATIONALS~~

The information contained in
this document will not be disclosed
to foreign nationals or their repre-
sentatives

~~SECRET~~

~~SECRET~~

THE
NATIONAL
COMMUNICATIONS SECURITY
MATÉRIEL PROGRAM

PART I - Current Equipments and Mid - Range
Development

PART II - Current Cryptomaterial Production

SEPTEMBER 1954

NATIONAL SECURITY AGENCY

~~SECRET~~

~~S E C R E T~~

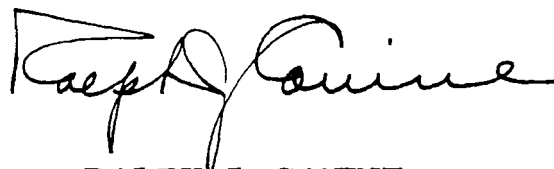
September 1954

FOREWORD

The Director, National Security Agency, has the responsibility for formulating, for consideration by the Board, integrated programs for the research, development, production, and procurement necessary to meet the requirements of the departments and agencies for crypto-equipments and materials.

In accordance with this responsibility, the program contained herein has been compiled by NSA and approved by the USCSB as a basis upon which to construct detailed implementation plans. For practical reasons, this initial statement is the current NSA program and does not reflect all of the special requirements of the civil agencies nor the production capacity of any agency other than NSA. Future statements of the program will be more comprehensive.

Comments and suggestions on the program content and presentation are welcome at any time.



RALPH J. CANINE
Lieutenant General, US Army
Director

~~S E C R E T~~

~~S E C R E T~~

INTRODUCTION

1 This program shows the principal requirements of the government for communications security materials, the NSA production capabilities available to meet them, and outlines the equipments available in production or under development to fulfill existing and projected needs. The program consists of three parts as follows:

- I Current Equipments and Mid-Range Development (1954-1959)
- II Current NSA Cryptomaterial Production (1954-1956)
- III Long Range Communications Security Equipment Plan (1954-1964)

2 The portion presented here consists of Parts I and II. Part III is in preparation and will be submitted when completed.

3 The program is based upon the assumptions that peacetime conditions will prevail, that the government will continue its present high level of international activity, support of international forces, and assistance to those countries opposed to communism, and that no significant change will be required in operations to absorb the initial impact of war.

4 The objectives of the program are:

- a To assure the production of the cryptomaterial required
 - (1) By departments and agencies for operating their com-

~~S E C R E T~~

~~S E C R E T~~

munications security programs.

- (2) To meet the U S share of international communications security requirements (NATO, U K , etc)
- b To build a reserve of both produced material and production capacity sufficient to meet the impact of full mobilization .
- c To develop or initiate the development of a minimum of one communications security equipment for each of the important methods of communication

~~S E C R E T~~

~~S E C R E T~~

PART I - CURRENT EQUIPMENTS AND MID - RANGE DEVELOPMENT

1 Communications security equipments are, of course, basic to NSA's program for providing overall support to the national communications security effort. The types of equipment currently in use and the extent of that usage determine directly the type and volume of keying material which must be procured. Similarly, the types of equipment currently under development determine the trend which that production will take in the future.

2 The current equipment and mid-range development program is shown in the following Chart I. It covers the principal equipments now in use and under development. It has been limited to equipments conceivably of use to both civil and military Federal agencies and departments. The chart, which is organized on the basis of the major communication fields in which security is needed, shows the equipment available or under development to fill the need, the principal types of using agencies, the echelons of usage, and its status during the 5-year period.

3 The detail of a typical program, and one of the principal current ones, for getting new equipment into use is shown in Chart II. This shows the planned rates for the production and distribution of new literal electro-mechanical crypto-equipments for all echelons (AFSAM 7

~~S E C R E T~~

~~S E C R E T~~

and AFSAM 47B) and the rotors used in them. Similar detailed charts will be added to the program as equipments progress from development to production.

~~S E C R E T~~

~~SECRET~~

CURRENT EQUIPMENT AND MID-RANGE DEVELOPMENT

CHART 1

EQUIPMENT	AUTHORIZED USERS	USAGE LEVEL	STATUS-FY				
			54	55	56	57	58
I. LITERAL (26-CHARACTER), OFF-LINE							
A. ELECTRO-MECHANICAL, KEYBOARD-OPERATED, TAPE PRINTING							
1. AFSAM 25 B, C (FIVE OR TEN 26-PT ROTOR WAZE, 97 LBS) FAIR LONG-TERM SECURITY	Civ & Mil (Intra, Joint, Combined, NATO)	Med, High	REPLACED BY AFSAM 7 AND 47B				
2. CSP 2500 (FIVE OR TEN 26-PT ROTOR WAZE, 37 LBS) FAIR TO HIGH LONG-TERM SECURITY DEPENDING ON MODE OF OPERATION	MIL (Intra, Joint)	Med, High	**				
3. CSP 850 (FIVE OR TEN 26-PT ROTOR WAZE, 37 LBS) FAIR TO HIGH LONG-TERM SECURITY DEPENDING ON MODE OF OPERATION	MIL (Intra, Joint, Combined)	Med, High	REPLACED BY AFSAM 7 AND 47B				
4. MEC-1 (FIVE OR TEN 26-PT ROTOR WAZE, 37 LBS) FAIR TO HIGH LONG-TERM SECURITY DEPENDING ON MODE OF OPERATION	CIVIL	Med, High	}				
5. AFSAM 7 (EIGHT 26-PT ROTOR WAZE, 38 LBS) HIGH SHORT-TERM TO HIGH LONG-TERM SECURITY DEPENDING ON MODE OF OPERATION	Civ & Mil (Intra, Joint, Combined, NATO)	Low, Med, High*	}				
6. AFSAM 47B (EIGHT 26-PT ROTOR WAZE, 45 LBS) HIGH SHORT-TERM TO HIGH LONG-TERM SECURITY DEPENDING ON MODE OF OPERATION	Civ & Mil (Intra, Joint, Combined, NATO)	Low, Med, High*	}				
B. MECHANICAL, TAPE PRINTING							
7. M-200/CSP 1500 (5 ROTORS, HAGELIN TYPE, 9 LBS) FAIR SHORT-TERM SECURITY	Civ & Mil (Intra, Joint)	Low	REPLACED BY AFSAM 7, 6, 30				
8. AFSAM 36 (12 ROTORS, HAGELIN TYPE, 10 LBS) FAIR SHORT-TERM SECURITY	Civ & Mil (Intra, Joint)	Low	}				
9. AFSAM 17 (ELEVEN 26-PT PNEUMATIC ROTOR WAZE, 10 LBS) HIGH SHORT-TERM TO HIGH LONG-TERM SECURITY DEPENDING ON MODE OF OPERATION	Civ & Mil (Intra, Joint, Combined)	Low, Med*	}				
10. AFSAM 21 (M-200/CSP 1500 MODIFIED FOR ONE-TIME TAPE, 9 LBS) HIGH LONG-TERM SECURITY	Civ & Mil (Intra, Joint)	Low, Med, High	}				
II. TELETYPE (32-CHARACTER), ON/OFF-LINE							
A. NON-SYNCHRONOUS FOR NETWORK OPERATION							
11. ASAM 2-1 (FIVE 26-PT ROTOR WAZE, 74 LBS) FAIR LONG-TERM SECURITY (ASAM 2-1 IS CURRENTLY BEING MODIFIED TO PROVIDE HIGH LONG-TERM SECURITY)	Civ & Mil (Intra, Joint, Combined)	Med, High	REPLACED BY AFSAM 9				
12. AFSAM 3A (MODIFIED SIGNIN) (EIGHT 26-PT ROTOR WAZE, SELF-CONTAINED KEYBOARD AND TAPE PRINTER, 252 LBS) HIGH LONG-TERM SECURITY	MIL (Intra)	Med, High	REPLACED BY AFSAM 9				
13. AFSAM 9 (NINE 26-PT ROTOR WAZE OR ONE-TIME TAPE UNIT, 40 LBS) HIGH SHORT-TERM OR LONG-TERM SECURITY DEPENDING ON MODE OF OPERATION	Civ & Mil (Intra, Joint, Combined)	Low, Med, High*	}				
14. AFSAM 3B (ELEVEN 26-PT ROTOR WAZE, SELF-CONTAINED KEYBOARD AND TAPE PRINTER, 252 LBS) HIGH LONG-TERM SECURITY	Civ & Mil (Intra, Joint)	Med, High	}				
B. SYNCHRONOUS, FOR POINT-TO-POINT OPERATION							
15. AFSAM 7315 (SINGLE CHANNEL, TAPE INPUT ONLY, USES AFSAM 9 WITH ROTOR WAZE OR TAPE UNIT, 210 LBS) HIGH LONG-TERM SECURITY	Civ & Mil (Intra, Joint, Combined)	Med, High	}				
16. AFSAM 2K (ELECTRONIC CRYPTO-UNIT, SINGLE CHANNEL, ACCEPTS INPUT FROM REMOTE TELEPRINTER, 250 LBS) HIGH LONG-TERM SECURITY	Civ & Mil (Intra, Joint)	High	}				
17. AFSAM 2D (ELECTRONIC CRYPTO-UNIT, MULTI-CHANNEL FOR USE WITH AFSAM 2C, 300 LBS) HIGH LONG-TERM SECURITY	Civ & Mil (Intra, Joint, Combined)	High	}				
18. AFSAM 2M (ELECTRONIC CRYPTO-UNIT, MULTI-CHANNEL FOR USE WITH AFSAM 2C AND SIMILAR WIRE-BASE EQUIPMENT, 250 LBS) HIGH LONG-TERM SECURITY	Civ & Mil (Intra)	Med, High	}				
C. SYNCHRONOUS, FOR FOX BROADCAST OPERATIONS							
19. AFSAM 37 (ELECTRONIC CRYPTO-UNIT, RECEIVE TERMINALS PROVIDED WITH SEMI-AUTOMATIC REAR FOR INDICATELY SYNCHRONIZING WITH TRANSMITTER, 250 LBS) HIGH LONG-TERM SECURITY	Civ & Mil (Intra, Joint, Combined)	Low, Med, High	}				
III. SPEECH							
A. NARROW BAND, FIXED PLANT							
20. AFSAY 300 (SINGLE CHANNEL, PUSH-TO-TALK SYSTEM FOR USE OVER COMMERCIAL WIRELINES, 300 LBS) HIGH LONG-TERM SECURITY	Civ & Mil (Intra, Joint)	Med, High	}				
B. WIDE BAND, FIXED PLANT							
21. AFSAY 501 (SINGLE CHANNEL, PUSH-TO-TALK SYSTEM FOR USE OVER BROAD WIRELINES, OR SPECIAL RADIO CIRCUITS, 300 LBS) HIGH LONG-TERM SECURITY	Civ & Mil (Intra, Joint)	Med, High	}				
22. AFSAY 507 (DUAL CHANNEL, FULL DUPLEX SYSTEM FOR USE OVER MICROWAVE RADIO LINKS, 1700 LBS) HIGH LONG-TERM SECURITY	Civ & Mil (Intra, Joint)	High	}				
C. NARROW BAND, MOBILE							
23. AFSAY 505 (SINGLE CHANNEL, FULL DUPLEX SYSTEM FOR USE OVER LAND LINES OR HF RADIO, 2300 LBS) HIGHEST LONG-TERM SECURITY	Civ & Mil (Intra, Joint)	Med, High	}				
D. WIDE BAND, MOBILE							
24. AFSAY 504(X-2) (SINGLE CHANNEL, PUSH-TO-TALK SYSTEM FOR VEHICULAR USE OVER TACTICAL VHF RADIO, 35 LBS) HIGH SHORT-TERM SECURITY	Civ & Mil (Intra, Joint, Combined)	Low, Med	}				
25. AFSAY 505 (SINGLE CHANNEL, PUSH-TO-TALK SYSTEM FOR AIRBORNE USE OVER VHF/UHF RADIO, 50 LBS) HIGH SHORT-TERM SECURITY	Civ & Mil (Intra, Joint, Combined)	Low	}				
IV. FACSIMILE							
A. FIXED PLANT, POINT-TO-POINT OPERATION							
26. AFSAX 500/AFSAJ 100 (SINGLE CHANNEL SYSTEM FOR USE OVER LONG WIRE LINES AND HF RADIO, 2500 LBS) HIGH SHORT-TERM SECURITY	Civ & US MIL (Intra)	Med, High	}				
27. AFSAX 505 (SINGLE CHANNEL SYSTEM FOR USE OVER SHORT WIRE LINES AND HF RADIO, AND WITH AUXILIARY EQUIPMENT OVER LONG WIRE LINES AND HF RADIO, 475 LBS) HIGH LONG-TERM SECURITY	Civ & Mil (Intra, Joint, Combined)	High	}				
B. Fixed Plant, FOX Broadcast Operation							
28. AFSAX 500 (FOR USE OVER LONG WIRE LINES AND HF RADIO, 300 LBS) HIGH LONG-TERM SECURITY	Civ & Mil (Intra, Joint, Combined)	Low, Med, High	}				
V. AIRCRAFT IDENTIFICATION							
29. REQUIREMENTS NOT YET FIRM. PRELIMINARY MODEL DEVELOPMENT SHOWN ON A HIGH SECURITY, COMPLETELY AUTOMATIC SYSTEM FOR USE WITH MARK X-177. BASIC RESEARCH CONTINUING ON MORE SOPHISTICATED SYSTEM.	MIL (Intra, Joint, Combined)	Low	}				
VI. GUIDED WEAPONS CONTROL							
30. REQUIREMENTS NOT YET SPECIFIED. IF SECURITY IS REQUIRED, WILL BE PROVIDED AS INTEGRATED PART OF COMMUNICATION CONTROL EQUIPMENT.	MIL	Low	}				

Research
 Development
 Production
 Usage
 Regional Usage

Research Evaluation of Most Current Methods Available to Develop New Systems.
 Development of Physical Equipment in accordance with expressed military characteristics and estimated security criteria.
Production Means that the item is in production to some extent to not increase to reflect quantity of production or distribution schedules.
Equipment in Service, but No Intended to Reflect Quantity.
Equipment Remaining in Limited Use Only.

* Usage Level Depends on Mode of Operation.

** Retained for High-Level Intra and Inter-US Use.

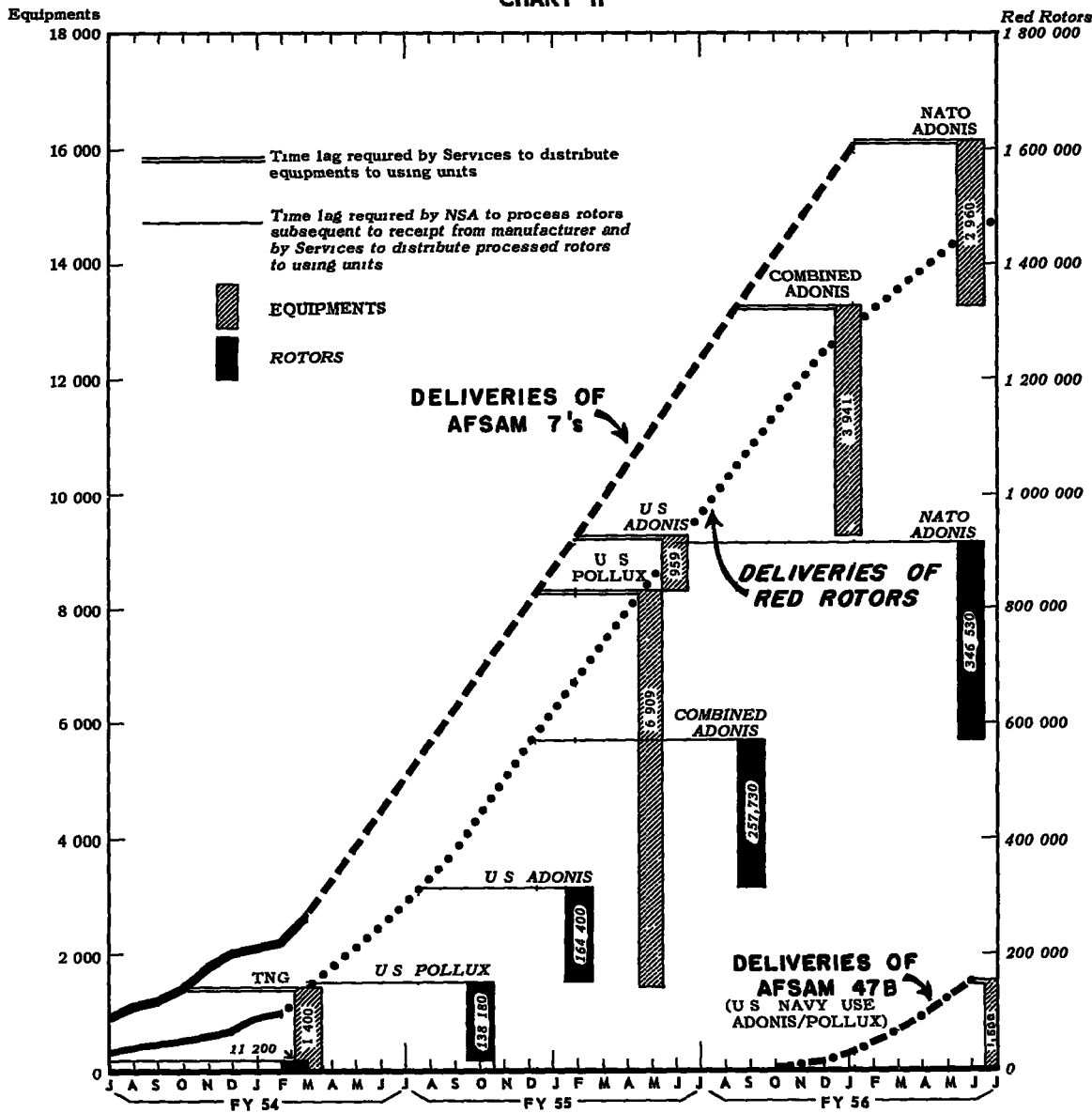
15 SEP 54
NSA 402

~~SECRET~~

~~SECRET~~

IMPLEMENTATION OF ADONIS/POLLUX PROGRAM

CHART II



15 SEP 54
NSA 402

~~SECRET~~

PART II - CURRENT CRYPTOMATERIAL PRODUCTION

1 PRODUCTION - The production of cryptomaterial to support the government's communications security activities constitutes a major segment of this program. The types of cryptomaterial which constitute the bulk of the production activity are one-time tapes (Chart III), one-time pads (Chart IV), rotors (Chart V), key list (Chart VI), codes (Chart VII), and instructional documents (Chart VIII).

2 Summarized, the situation is

a All operating requirements placed on NSA are met from production capacity currently available to NSA.

b Cryptomaterial for mobilization reserve requirements placed on NSA is being produced by NSA and will be maintained during the 5-year period to meet varying requirements. Increases in production capacity are planned mainly by improvements in methods and production equipment, and in utilization of plant capacity.

NOTE 1 Operating requirements included in the following charts indicate that material requested of NSA to meet the current needs of the various U S Departments and Agencies as well as those international requirements for which NSA is responsible.

2 The Mobilization Reserve requirement is based on the

~~SECRET~~

~~S E C R E T~~

mobilization needs of the users and the ability of NSA to meet these needs, i e , a stock-pile of keying material to assure a continual supply of materials from M-Day to P-Day (P-Day being "production day" or that time when it is anticipated that war time needs can be met on a current basis) Mobilization reserves of cryptomaterials produced differ in each case due to operating requirements, planned rate of supersession, and probability of compromise The Mobilization Reserve requirement, together with the Operating requirement, comprises the Total requirement indicated on the charts.

3 The Planned Production indicated is based on a gradual buildup in those areas where a mobilization reserve is considered necessary with a goal of attaining this point at the earliest practicable date and, from there on, maintaining a level of production to provide the needs of the consumers on a current basis

3 These charts cover those requirements for cryptomaterial requested of NSA and the NSA production available to meet them. However, a detailed survey of all U S requirements for cryptomaterial, as well as all production capacity available to the U S ,

~~S E C R E T~~

~~S E C R E T~~

is being made The next revision of the program will indicate total requirements and total U S production capacity available It is planned, to then prepare, for national emergency use, a method for utilizing any production capacity which is in excess of a user's internal requirements

~~S E C R E T~~

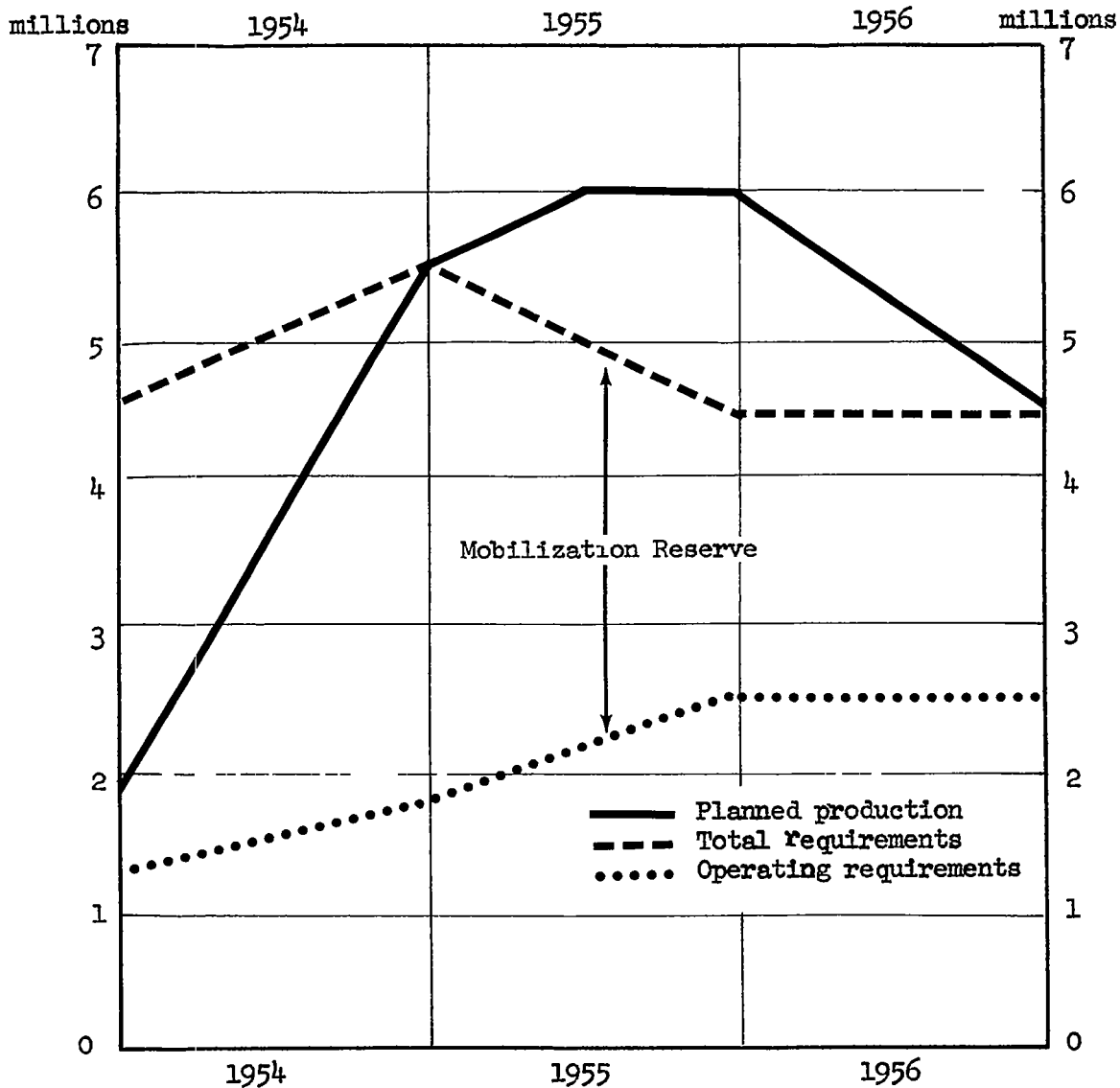
~~S E C R E T~~

ESTIMATED TOTAL REQUIREMENTS AND PLANNED

NSA PRODUCTION OF ONE-TIME TAPES

(Expressed In Terms Of 3" Rolls)

CHART III A



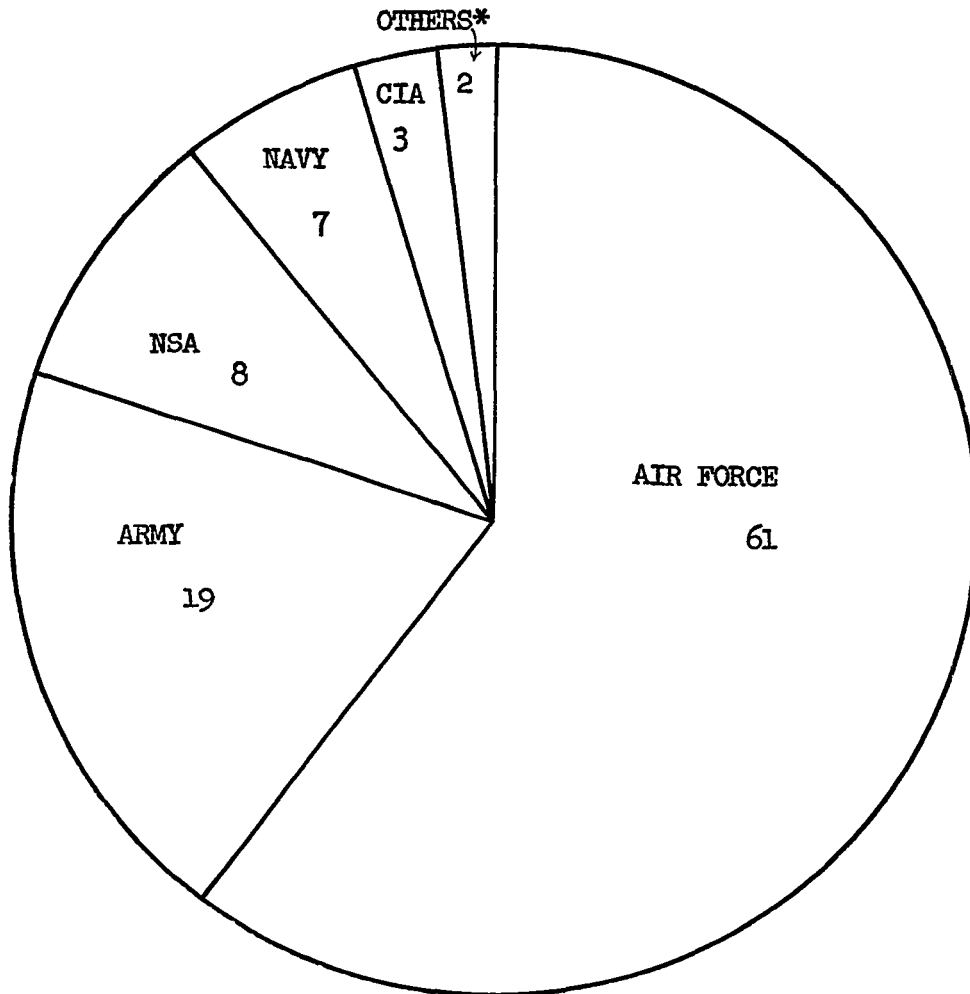
15 SEP 54
NSA 402

~~S E C R E T~~

NSA FY-54 PERCENTAGE DISTRIBUTION OF ONE-TIME TAPES

(Expressed In Terms Of 3" Rolls)

CHART III B



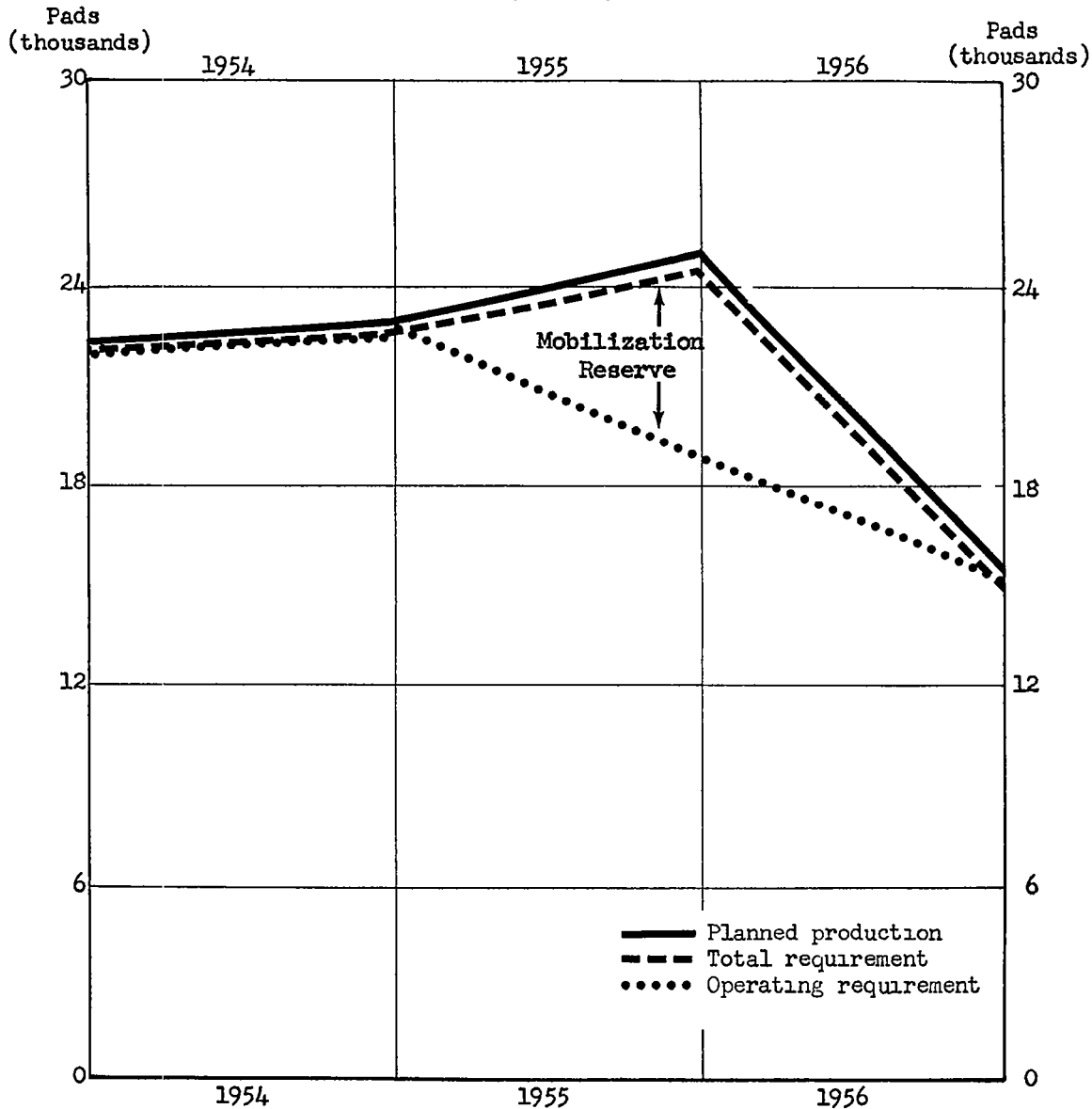
*OTHERS include NATO, AEC, Etc.

15 SEP 54
NSA 402

~~SECRET~~

ESTIMATED TOTAL REQUIREMENTS AND PLANNED NSA PRODUCTION
OF ONE-TIME PADS (ALL TYPES)

CHART IV A

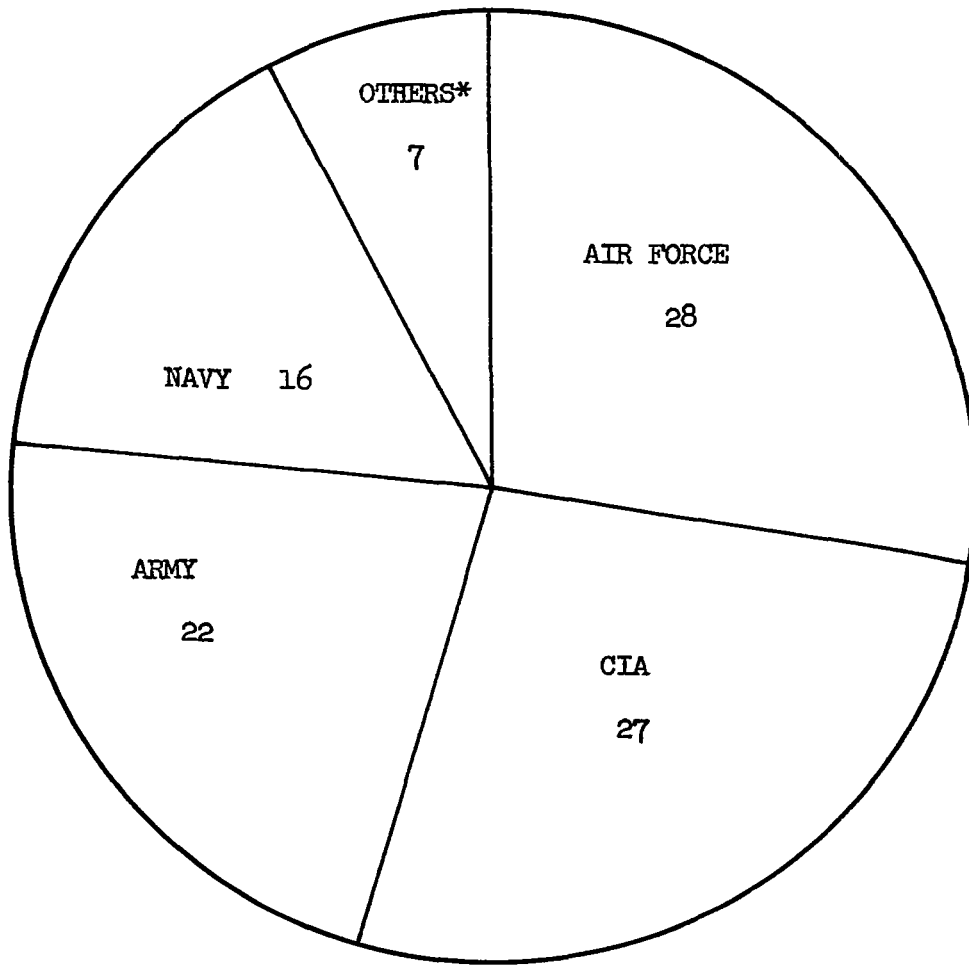


15 SEP 54
NSA 402

~~SECRET~~

~~S E C R E T~~

NSA FY-1954 PERCENTAGE DISTRIBUTION OF
ONE-TIME PADS
CHART IV B



*OTHERS include AEC, NSA, WEATHER BUREAU, NATO, Etc.

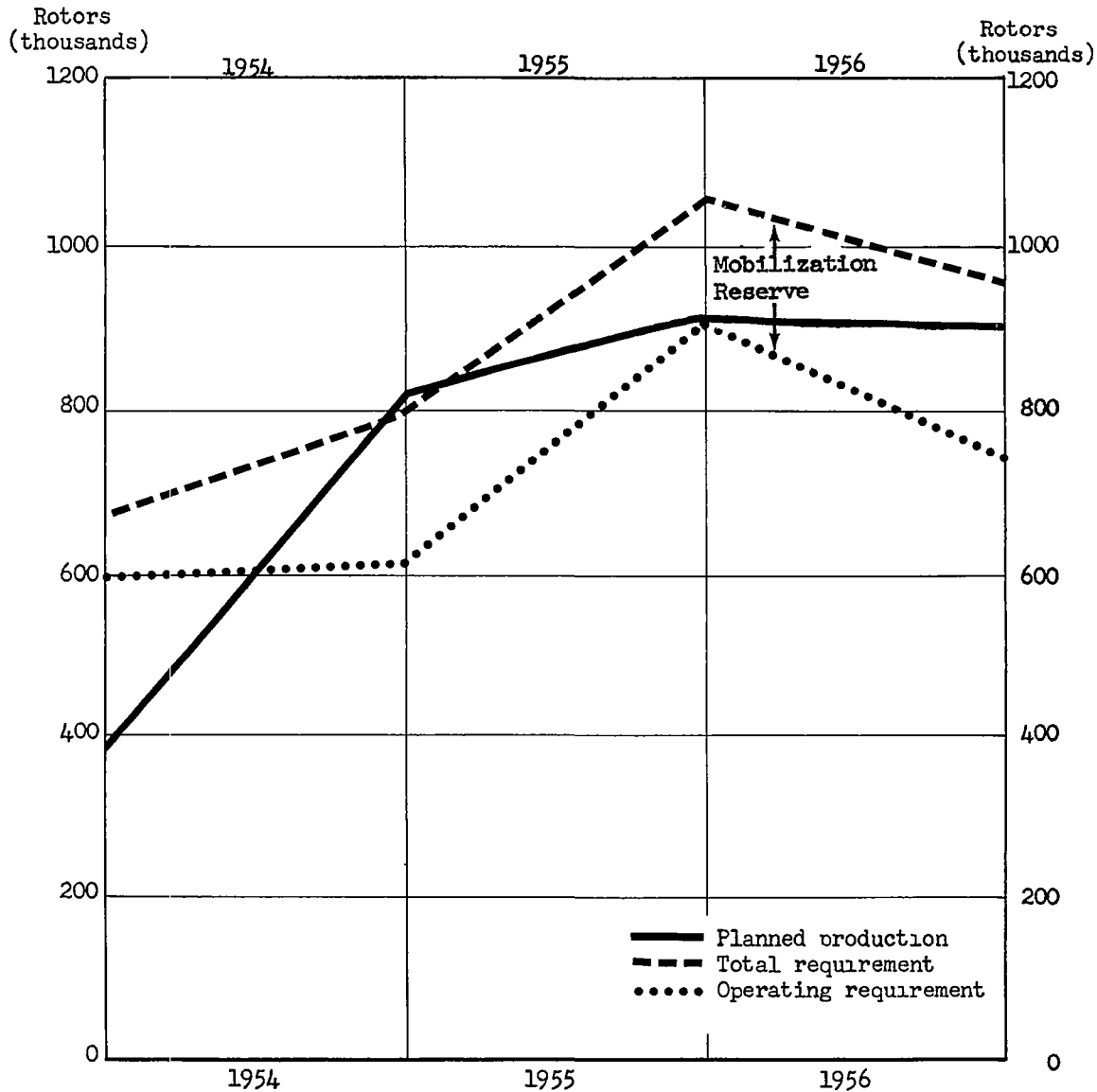
15 SEP 54
NSA 402

~~S E C R E T~~

~~SECRET~~

ESTIMATED TOTAL REQUIREMENTS AND PLANNED NSA PRODUCTION OF ROTORS (ALL TYPES)

CHART V A



15 SEP 54
NSA 402

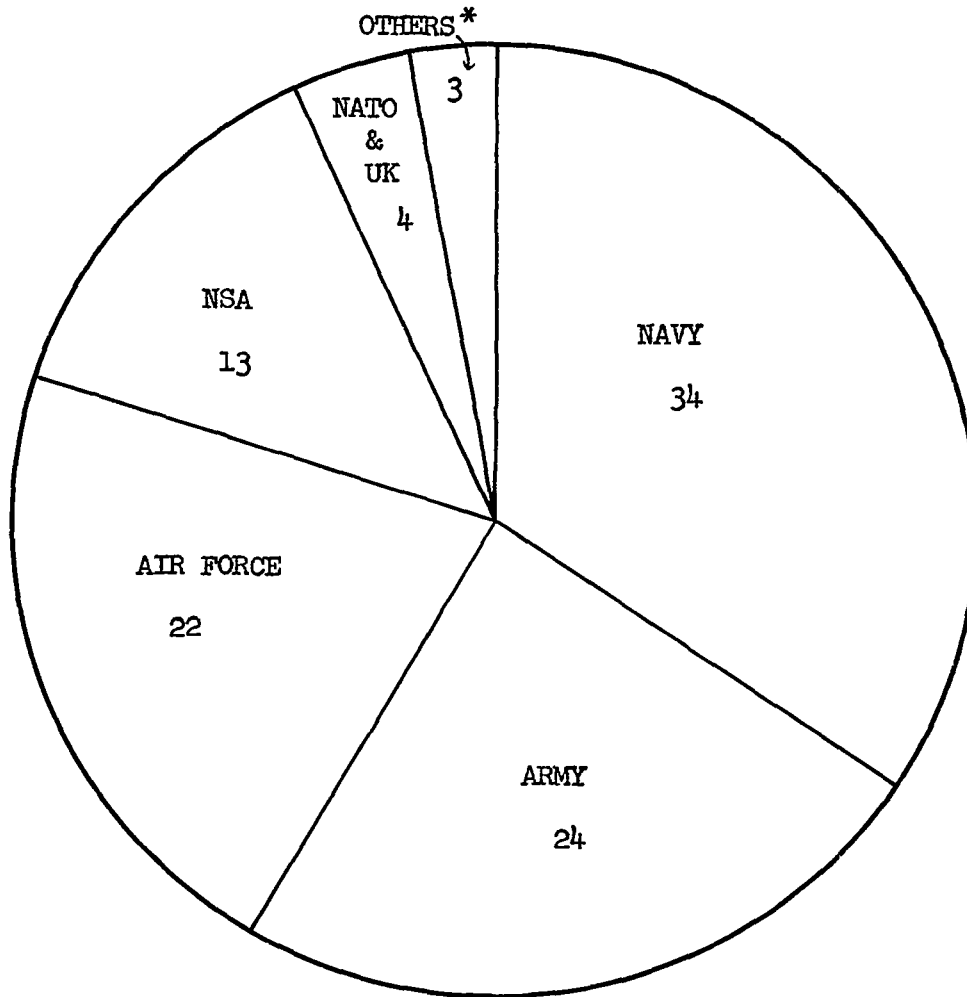
~~SECRET~~

~~S E C R E T~~

NSA FY-54 PERCENTAGE DISTRIBUTION OF ROTORS

(ALL TYPES)

CHART V B



* OTHERS include CIA, FBI, STATE, Etc.

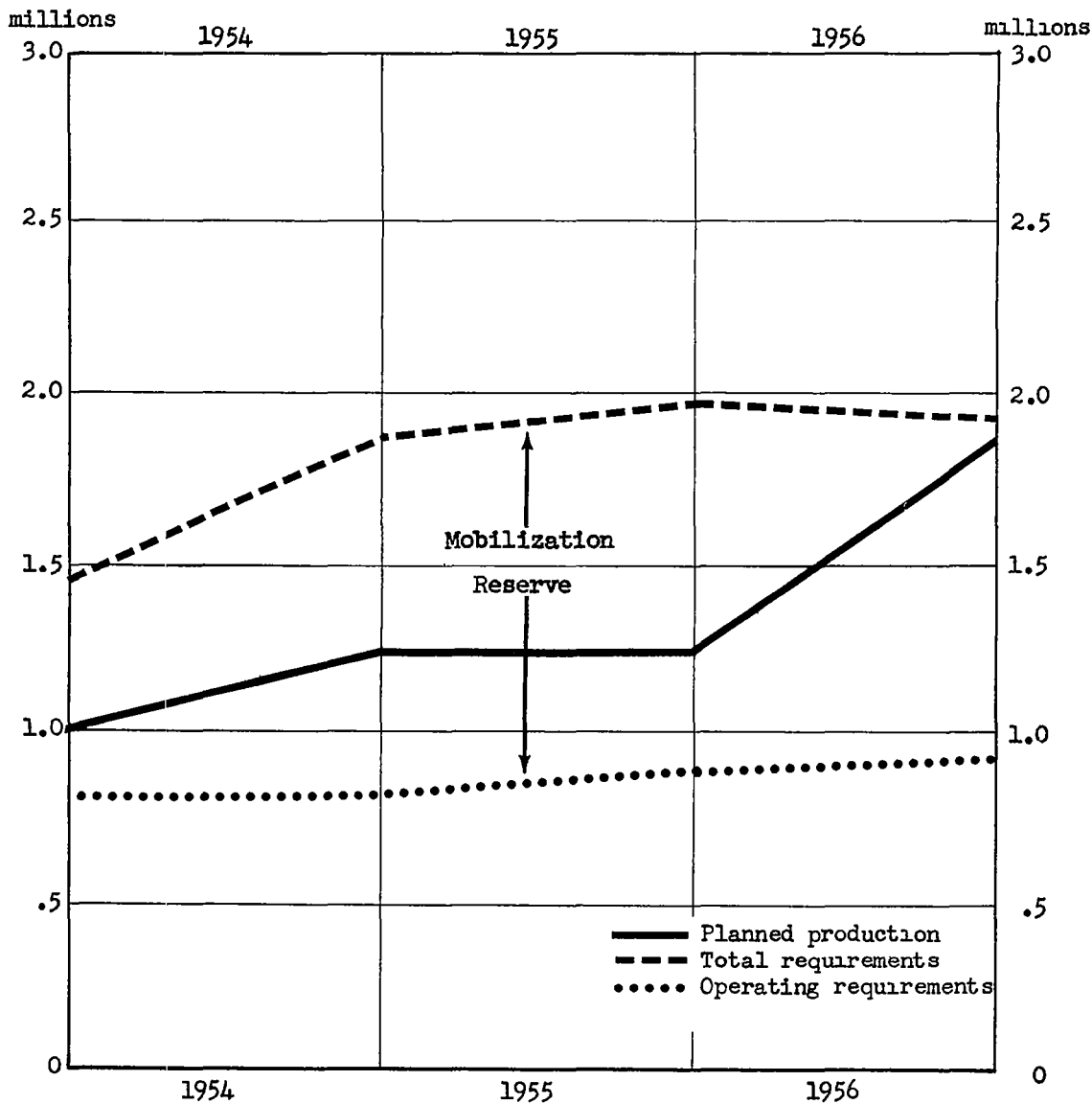
15 SEP 54
NSA 402

~~S E C R E T~~

~~S E C R E T~~

ESTIMATED TOTAL REQUIREMENTS AND PLANNED NSA PRODUCTION OF KEY LISTS
(Expressed in Terms of 3 Page Documents)

CHART VI A



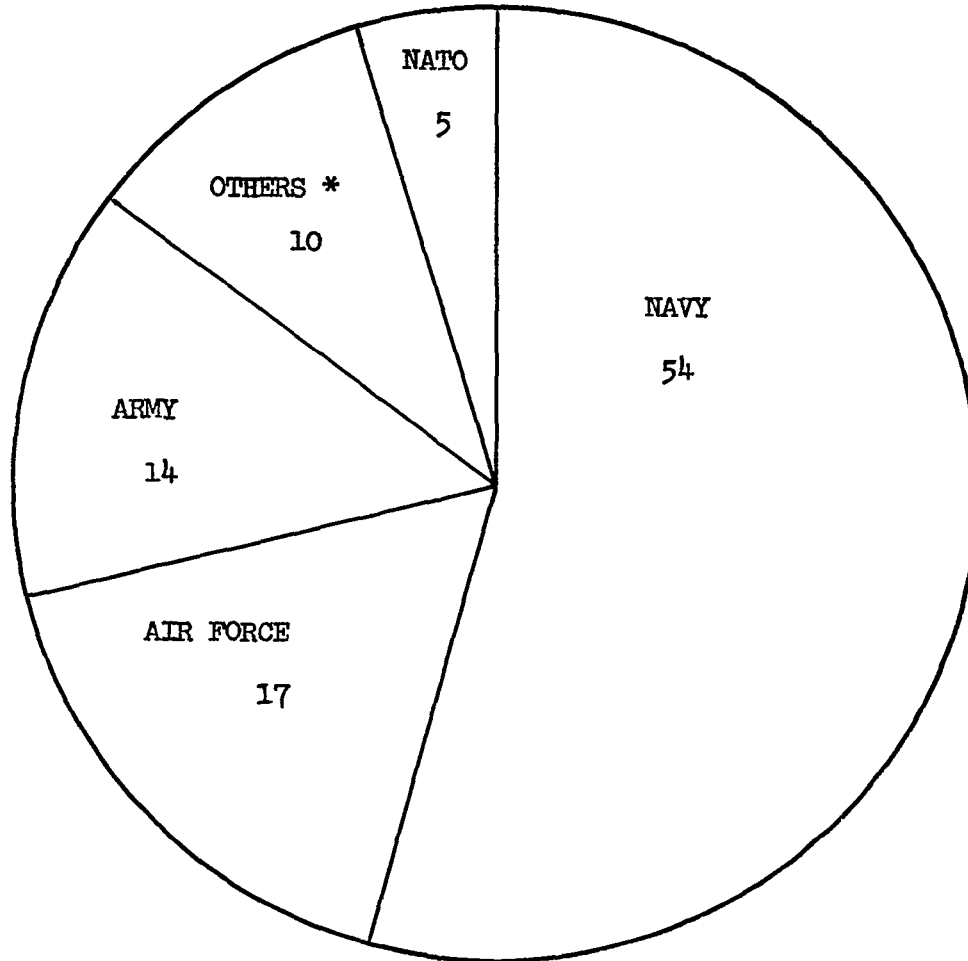
15 SEP 54
NSA 402

~~S E C R E T~~

~~S E C R E T~~

NSA FY-1954 PERCENTAGE DISTRIBUTION OF KEY LISTS

CHART VI B



* OTHERS include CIA, NSA, UK, Etc.

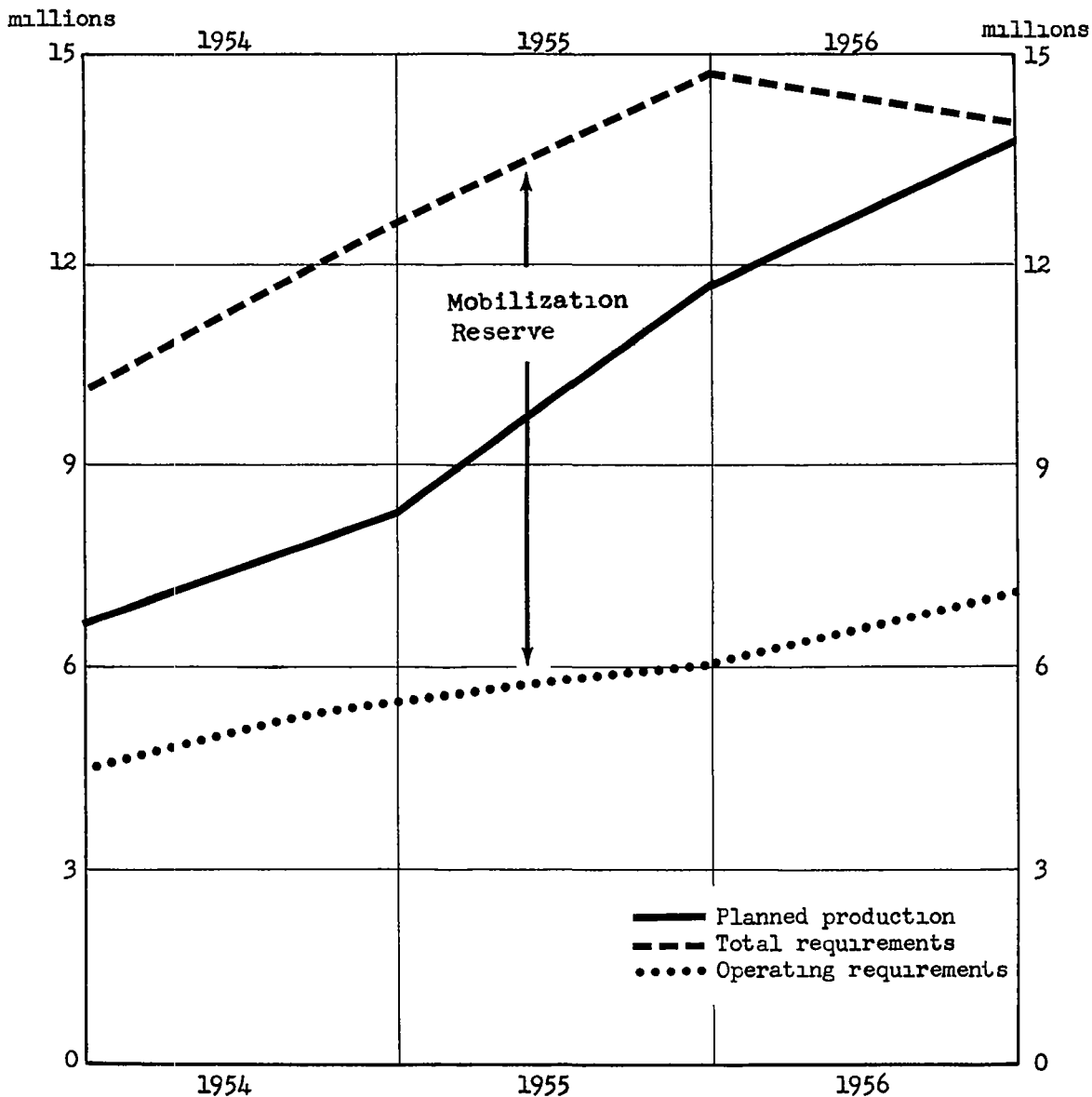
15 SEP 54
NSA 402

~~S E C R E T~~

~~S E C R E T~~

ESTIMATED TOTAL REQUIREMENTS AND PLANNED NSA PRODUCTION OF CODES
(Expressed in Terms of 16 Page Documents)

CHART VII A



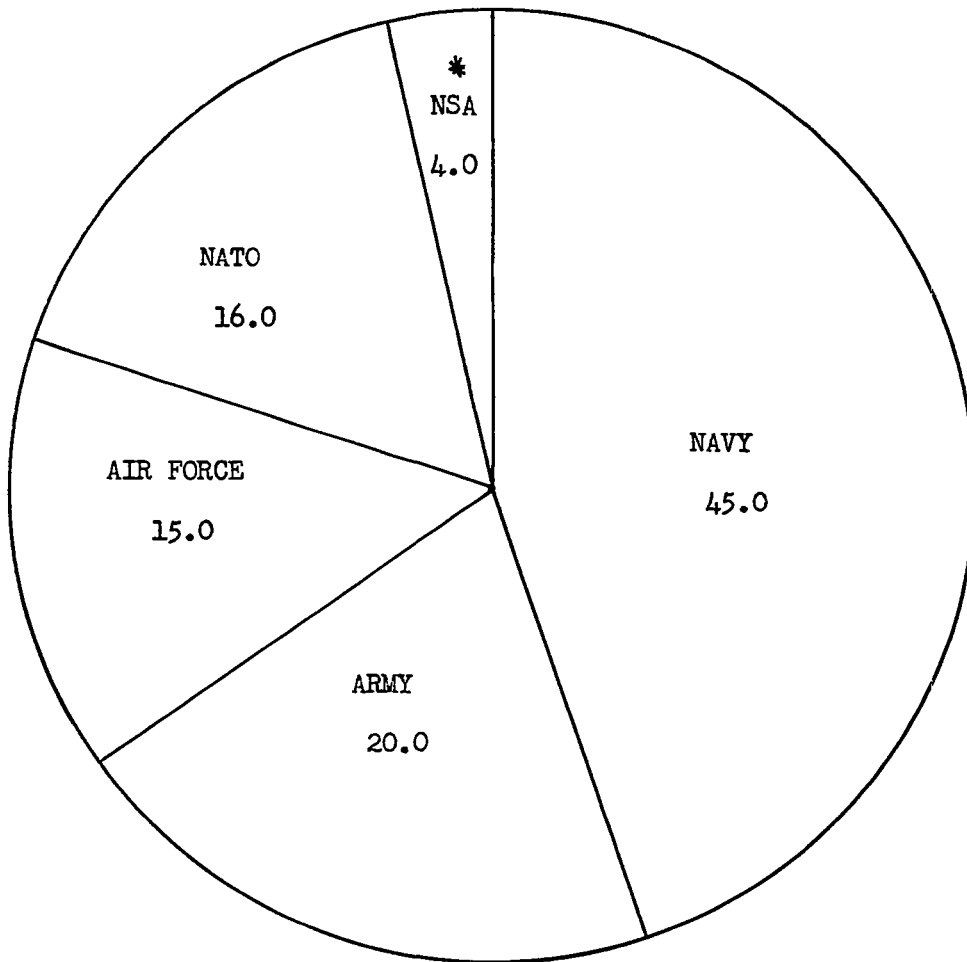
15 SEP 54
NSA 402

~~SECRET~~

NSA FY-54 PERCENTAGE DISTRIBUTION

OF CODES

CHART VII B



* Held for Operational Reserve

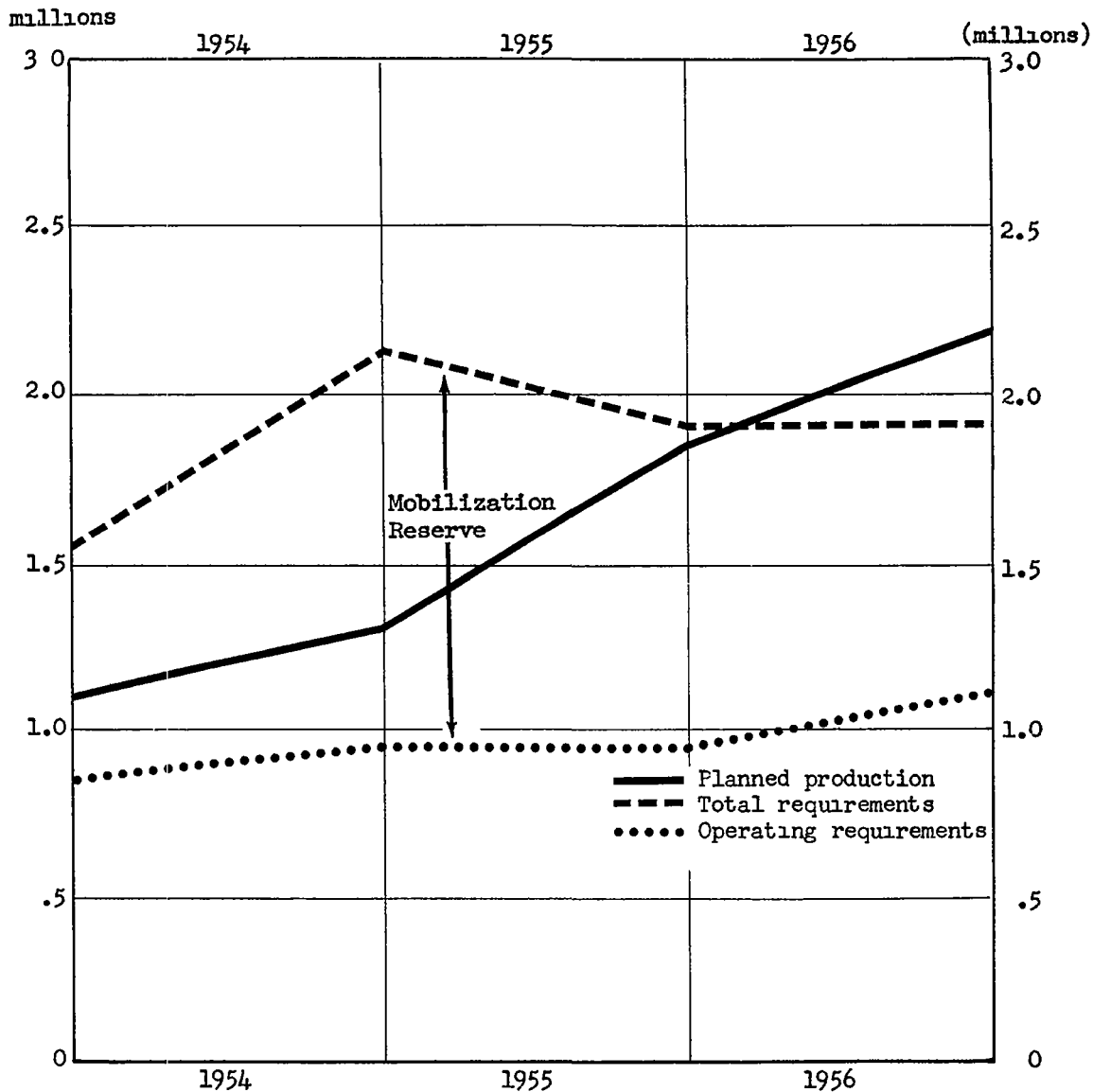
15 SEP 54
NSA 402

~~SECRET~~

~~SECRET~~

ESTIMATED TOTAL REQUIREMENTS AND PLANNED NSA PRODUCTION
OF GENERAL INSTRUCTIONAL DOCUMENTS
(Expressed in Terms of 32 Page Documents)

CHART VIII A

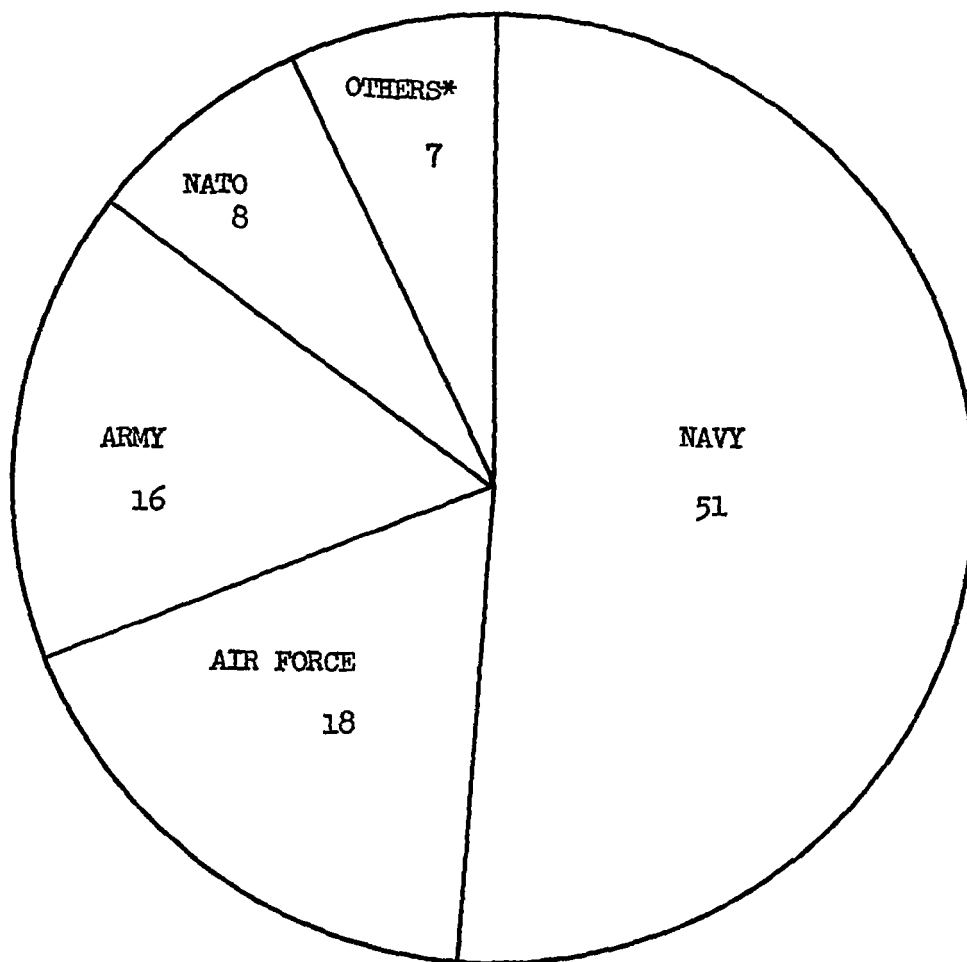


15 SEP 54
NSA 402

~~S E C R E T~~

NSA FY-1954 PERCENTAGE DISTRIBUTION
OF GENERAL INSTRUCTIONAL DOCUMENTS

CHART VIII B



*OTHERS INCLUDE FBI, AEC, CIA, NSA, Etc.

15 SEP 54
NSA 402

~~S E C R E T~~