

WITHDRAWAL SHEET (PRESIDENTIAL LIBRARIES)

FORM OF DOCUMENT	CORRESPONDENTS OR TITLE	DATE	RESTRICTION
#1 memo	NSAM 315 open 6-26-98 S 1 p	10/29/64	A
#2 rpt	Status of NSAM 315 survey C 1 p <i>open 4.14.05</i>	5/3/65	A
#2a memo	Gordon to President TS 2 p <i>open 3/12/08 NLJ/RAC 05-48</i>	4/30/65	A
#2b rpt	Summary Report TS 41 p <i>sanitized 12/10/11 per NLJ/RAC 5-47</i>	4/30/65	A
#3 rpt	Survey of Technical and Physical... S 41 p <i>sanitized 12/10/11 per NLJ/RAC 5-47</i>	4/23/65	A
#4 memo	Chase to Bundy S 1 p <i>open 4.14.05</i>	5/6/65	A
#5 rpt	Duplicate of #2 <i>open 4.14.05</i>		
#6 memo	Bundy to Valenti C 1 p <i>open 4.14.05</i>	4/30/65	A
#7 rpt	Duplicate of #2b		
#8 rpt	Duplicate of #2a <i>open 3/12/08 NLJ/RAC 05-48</i>		
#9 memo	Clark to Chase TS 1 p <i>open 4.14.05</i>	4/22/65	A
#9a rpt	Attachment to #9 C 1 p <i>open 4.14.05</i>	undated	A
#9b rpt	Attachment to #9 S 1 p <i>open 4.14.05</i>	4/14/65	A
#10a rpt	Duplicate of #9b <i>open 4.14.05</i>		
#12 rpt	Survey of Technical and Physical... S 86 p <i>sanitized 12/10/11 per NLJ/RAC 5-47</i>	4/7/65	A

FILE LOCATION

NSF, NSAM, NSAM 315--Communications Security Survey

Box 5

RESTRICTION CODES

- (A) Closed by Executive Order 12356 governing access to national security information.
 (B) Closed by statute or by the agency which originated the document.
 (C) Closed in accordance with restrictions contained in the donor's deed of gift.

WITHDRAWAL SHEET (PRESIDENTIAL LIBRARIES)

FORM OF DOCUMENT	CORRESPONDENTS OR TITLE	DATE	RESTRICTION
#14 rpt	Survey of Technical and Physical... S 84 p	4/7/65	A
#15 rpt	Agenda for meeting with Mr. Smith C 1 p <i>open 4.14.05</i>	undated	A
#20 memo	Chase to Bundy S 1 p <i>open 4.14.05</i>	3/12/65	A
#21 memo	Chase to Valenti S 1 p <i>open 4.14.05</i>	3/11/65	A
#22a memo	Staats to Bundy S 1 p <i>open 3/12/08 NLJ/RAC 05-48</i>	3/2/65	A
#23 memo	Chase to Bundy (page 2) TS 1 p <i>OPEN 9.14.05 NLJ 05-67</i>	3/2/65	A
#24a memo	Chase to Valenti S 3 p <i>3/11/72 ED 2.14.05 NLJ 05-67</i>	3/1/65	A
#25 memo	Chase to Clark S 1 p <i>open 4.14.05</i>	3/1/65	A
#26 memo	Duplicate of #24a		
#31 memo	Chase to Valenti S 1 p <i>open 4.14.05</i>	2/25/65	A
#32 memo	Chase to Bundy S 1 p <i>open 4.14.05</i>	2/17/65	A
#33 memo	Chase to Bundy S 1 p <i>open 3/12/08 NLJ/RAC 05-48</i>	2/10/65	A
#33a memo	White House Communication Study PCI 1 p <i>open 3/12/08 NLJ/RAC 05-48</i>	2/10/65	A
#34 rpt	White House and EOB Telephone Survey PCI 2 p <i>open 3.16.06 NLJ 05-69</i>	2/8/65	A

FILE LOCATION

NSF, NSAM, NSAM 315--Communications Security Survey

Box 5

RESTRICTION CODES

- (A) Closed by Executive Order 12356 governing access to national security information.
 (B) Closed by statute or by the agency which originated the document.
 (C) Closed in accordance with restrictions contained in the donor's deed of gift.

WITHDRAWAL SHEET (PRESIDENTIAL LIBRARIES)

FORM OF DOCUMENT	CORRESPONDENTS OR TITLE	DATE	RESTRICTION
#35a memo	C&P to Sampson PCI 5 p <i>open 3.16.06 NW 05.69</i>	11/12/64	A
#38 memo	Clark to Chase C 1 p <i>open 4.14.05</i>	2/1/65	A
#39a memo	Carey to Bundy S 4 p <i>open 3/12/08 NJ/RAC 05-48</i>	1/22/65	A
#40 memo	Carey to Bundy S 4 p <i>open 3.16.06 NW 05.69</i>	1/21/65	A
#41 memo	Clark to Chase S 2 p <i>open 4.14.05</i>	1/12/65	A
#41a memo	Duplicate of #41		
#41b memo	Chase to Valenti S 1 p	1/9/65	A
#41e memo	Carey to Bundy S 1 p	1/8/65	A
#42 memo	Duplicate of #41b		
#42a memo	Duplicate of #41c		
#43 memo	Duplicate of #41b		
#44 memo	Duplicate of #41c		
#46 memo	Chase to Bundy S 1 p	12/19/64	A
#46b memo	NSAM 315 <i>agen 6-26-98</i> S 1 p	10/29/64	A
#46d rpt	"Procedure and Conducting..." S 4 p <i>open 3.16.06 NW 05.69</i> <i>dup. #41a, this file</i>	11/5/64	A

FILE LOCATION

NSF, NSAM, NSAM 315--Communications Security Survey

Box 5

RESTRICTION CODES

- (A) Closed by Executive Order 12356 governing access to national security information.
 (B) Closed by statute or by the agency which originated the document.
 (C) Closed in accordance with restrictions contained in the donor's deed of gift.

WITHDRAWAL SHEET (PRESIDENTIAL LIBRARIES)

FORM OF DOCUMENT	CORRESPONDENTS OR TITLE	DATE	RESTRICTION
#46f rpt	"Survey of Physical Security..." S 3 p <i>open 3/12/08 NLJ/RAC 05-48</i>	12/18/64	A
#48 memo	Duplicate of #46f <i>open 3/12/08 NLJ/RAC 05-48</i>		
#49a memo	Duplicate of #46d		
#51 memo	Chase to Bundy S 1 p <i>open 4.14.05</i>	10/27/64	A
#52 memo	NSAM draft <i>sanitized 4.14.05</i> S 2 p	10/27/64	A
#53 memo	Gordon to Bundy S 1 p <i>open 4.14.05</i>	10/27/64	A
#54a memo	Chase to Bundy S 1 p	11/6/64	A
#55 memo	Duplicate of #54a		
#55 memo	Duplicate of #54a		
#55d memo	NSAM 315 <i>open 6-26-98</i> S 1 p	10/29/64	A
#55f memo	Bundy to President S 1 p <i>open 4.14.05</i>	11/6/64	A

FILE LOCATION

NSF, NSAM, NSAM 315--Communications Security Survey

Box 5

RESTRICTION CODES

- (A) Closed by Executive Order 12356 governing access to national security information.
- (B) Closed by statute or by the agency which originated the document.
- (C) Closed in accordance with restrictions contained in the donor's deed of gift.

THE WHITE HOUSE

WASHINGTON

~~SECRET~~

DECLASSIFIED

Authority NSC memo 4-13-98

By isa, NARA, Date 6-24-98

October 29, 1964

NATIONAL SECURITY ACTION MEMORANDUM NO. 315

MEMORANDUM FOR THE DIRECTOR OF THE BUREAU OF
THE BUDGET

SUBJECT: Survey of Physical Security Arrangements and Audio
Surveillance Countermeasures Covering the White House

1. The President has asked that you study the organization and effectiveness of (a) physical security arrangements in the White House and (b) the measures to counter audio-surveillance penetrations of the White House, including all voice facilities used by the President and the White House staff.
2. The study is to be made in collaboration with the Director of the Office of Science and Technology. You may call upon other Government agencies and special interagency groups (e. g., the NSC Special Committee on Technical Surveillance Countermeasures) for technical and non-technical advice and assistance.
3. The report to the President, to be completed by March 1, 1965, will be sent by this office to the President's Committee on the Warren Report for any comments and recommendations it may wish to make to the President.

McGeorge Bundy

McGeorge Bundy

cc: Secretary of State
Secretary of Defense
Secretary of the Treasury
Attorney General
Director of Central Intelligence
Director of the Office of Science
and Technology

bcc: Mr. Bundy ✓
Mr. Moyers ✓
Maj. Gen. Clifton ✓
C. O. White House
Communications
Mr. Hopkins ✓
Mr. Chase
NSC Files
L. JOHNSON

Dispatched 10/30/64
Repts Nos. 641-647

~~SECRET~~

~~CONFIDENTIAL~~

2
May 3, 1965

STATUS OF NSAM 315 SURVEY

	<u>Director's Memorandum</u>	<u>Summary Report</u>	<u>Complete set including chapters</u>
Original	President		
Courtesy (Copy 1)	President	President	
Copy 2	Director	Director	
Copy 3	Mr. Bundy		Mr. Bundy
Copy 4	Mr. Chase		Mr. Chase
Copy 5	Mr. Chase	Mr. Chase	
Copy 6	Mr. Chase	Mr. Chase	
Copy 7	Mr. Chase	Mr. Chase	
Copy 8	Dr. Hornig		Dr. Hornig
Copy 9	Mr. Carey/ Director		Mr. Carey/ Director
Copy 10	J. W. Clark		J. W. Clark
Copy 11	J. W. Clark	Mr. Chase	
Copy 12		Mr. Chase	
Copy 13		Mr. Chase	
Copy 14		Mr. Chase	
Copy 15		Mr. Chase	

Determined to be an
administrative marking

By jc On 3-18-05

~~CONFIDENTIAL~~

Distribution of #1831 (attached)

~~TOP SECRET~~

1831

EXECUTIVE OFFICE OF THE PRESIDENT
BUREAU OF THE BUDGET
WASHINGTON 25, D.C.

2a

APR 30 1965

MEMORANDUM FOR THE PRESIDENT

Subject: White House Security Survey

We have completed the survey of technical and physical security protection for the Presidency in accordance with NSAM 315. The survey covers arrangements for protecting the White House and, to a lesser extent, the ranch and the Executive Office Building, against possible technical penetrations, i.e., invasions of privacy and security through clandestine eavesdropping devices and telephone taps.

I have been quite disturbed to discover the existence of so many weaknesses in present security arrangements at the White House and the consequent exposure of your security and communications to technical penetration. Fundamental to this condition is the lack of clear responsibility or decision points for these matters.

The report identifies measures which should be taken, now and over a longer period, to tighten up and improve the security of the White House. I strongly recommend that you personally read the summary report.

In the survey, we have given careful attention to costs as well as benefits of the proposed improvements. I am satisfied that costs of actions growing out of the survey can be covered by appropriations available to appropriate agencies (primarily Defense and Treasury) in FY 1966.

Our general ground rules were to effect security improvements as the survey progressed, and examples of such improvements are noted in the attachment. However, fundamental improvements must await White House decision.

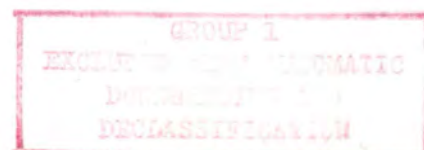
Mr. Bundy and I are ready at any time to discuss these matters and appropriate steps to carry out your decisions.

(signed) Kermit Gordon
KERMIT GORDON
Director

Attachment

DECLASSIFIED
E.O. 13292, Sec. 3.5
NLJ/RAC 05-48
By isl, NARA, Date 3-4-08

~~TOP SECRET~~



~~TOP SECRET~~AttachmentEXAMPLES OF SECURITY IMPROVEMENTS
MADE IN THE COURSE OF THE NSAM 315 SURVEY

1. Fundamental reductions have been made in possible compromising radiations from communications equipment handling classified material at the White House and the LBJ ranch.
2. Private line service to Mr. McNamara's residence from the White House switchboard has been rerouted.
3. Steps have been taken to design and fabricate transportable cryptographic communications equipment with reduced radiation levels which could accompany the President on trips, particularly abroad.
4. The C&P Telephone Company, in connection with certain new installations, is installing shielded cables direct from telephones in the West Wing to a consolidated terminal room now planned for construction.
5. White House police are now being taken to State for briefings in the audio surveillance threat and countermeasures.
6. The Secret Service has installed alarms in telephone terminal areas and other sensitive areas.
7. A better understanding of the technical penetration problems in the telephone companies has come about through very helpful discussions with representatives of AT&T, Chesapeake and Potomac, and Southwestern Bell, and those companies are considering development of technical features which would increase telephone security and privacy.
8. About 3,000 feet of surplus wire not needed for present service has been removed in the course of the special counter audio survey.

~~TOP SECRET~~

M-50/65-TS/7
C.5

2b

~~TOP SECRET~~

SUMMARY REPORT

SURVEY OF TECHNICAL AND PHYSICAL SECURITY PROTECTION
FOR THE PRESIDENCY

NSAM 315 Survey

April 30, 1965

~~TOP SECRET~~

SANITIZED
E.O. 13526, Sec. 3.5
NLJ/RAC 05-47
By isl NARA, Date 12-6-11

E.O. 12958
3.3 (b) (1)
6.2 (c)

THE WHITE HOUSE
WASHINGTON

~~SECRET~~

October 29, 1964

NATIONAL SECURITY ACTION MEMORANDUM NO. 315

MEMORANDUM FOR THE DIRECTOR OF THE BUREAU OF
THE BUDGET

SUBJECT: Survey of Physical Security Arrangements and Audio
Surveillance Countermeasures Covering the White House

1. The President has asked that you study the organization and effectiveness of (a) physical security arrangements in the White House and (b) the measures to counter audio-surveillance penetrations of the White House, including all voice facilities used by the President and the White House staff.
2. The study is to be made in collaboration with the Director of the Office of Science and Technology. You may call upon other Government agencies and special interagency groups (e. g., the NSC Special Committee on Technical Surveillance Countermeasures) for technical and non-technical advice and assistance.
3. The report to the President, to be completed by March 1, 1965, will be sent by this office to the President's Committee on the Warren Report for any comments and recommendations it may wish to make to the President.

McGeorge Bundy
McGeorge Bundy

cc: Secretary of State
Secretary of Defense
Secretary of the Treasury
Attorney General
Director of Central Intelligence
Director of the Office of Science
and Technology

~~SECRET~~

~~SECRET~~

Attachment A -
Summary Report

NSAM 315 SURVEY

Members of Steering Group:

NSA	Leo Rosen - Asst. Director for Research and Engineering
NSA	Raymond T. Tate - Chief, Radiation Engineering Section, Division of Communications Security
CIA	[REDACTED]
CIA	[REDACTED]
State	G. Marvin Gentile - Deputy Assistant Secretary for Security
Defense	Joseph A. Califano, Jr. - Special Assistant to the Secretary of Defense
OST	David Z. Robinson - Technical Specialist, Office of Science and Technology
BOB	James W. Clark - Assistant Division Chief (Air Force), Military Division

Consultants:

MIT	Jerome B. Wiesner - Dean of Science, Massachusetts Institute of Technology
Bell Lab	William O. Baker - Vice President (Research)
Bell Lab	Edward M. David - Research
AT&T	Richard T. James - Transmission Systems Engineer
CIA	[REDACTED]
FIAB	J. Patrick Coyne - Executive Secretary, President's Foreign Intelligence Advisory Board

Study participants:

DTM	Ralph L. Clark - Deputy to Director of Telecommunications Management
State	Charles D. Skippon - Deputy Chief, Domestic Operations Division, Office of Security
GSA	David B. Hall - Director of Planning Division, Office of Communications
NSA	[REDACTED] - Chief, Telephone Engineering Group, Office of Telecommunications
NSA	[REDACTED] - Technician, Radiation Engineering Section, Division of Communications Security
Defense	John T. McEvoy - Office of Special Assistant to the Secretary of Defense
State	Stanley E. Holden - Chief, Technical Security Branch of Domestic Operations, Office of Security

~~SECRET~~

~~TOP SECRET~~

TABLE OF CONTENTS

	<u>Page</u>
I. Introduction - The Problem -----	1
Basic Factors and Premises -----	1
Basic Conditions at the White House -----	2
Objectives and Approach of the Survey -----	5
II. Assessment of Risks and Vulnerabilities -----	7
III. Major Conclusions and Recommendations Pertaining to General Security and Audio Countermeasures	
Overall Security Responsibility -----	14
Audio Countermeasures Program -----	15
Security Aspects of Construction and Repair Activities -----	19
Personnel Clearances and Control of People -----	20
Classified Document Handling -----	22
Other Technical and Physical Security Measures -----	25
IV. Major Conclusions and Recommendations with Respect to Telephones and Communications -----	26
Need for Overall Responsibility -----	26
Planning for a New, More Secure System -----	28
Crypto-Secure Telephones -----	30
Responsibility for Telephone Security at the White House -----	31
Other Telephone Recommendations -----	33

~~TOP SECRET~~

~~TOP SECRET~~

	<u>Page</u>
Compromising Radiations (TEMPEST) -----	34
White House Office Machines -----	35

Detailed Reports

Chapter One: Audio Surveillance Countermeasures

Chapter Two: Telephone Security and Privacy

Chapter Three: Compromising Emanations from Secure Communications

Chapter Four: Handling and Control of Classified Documents

Chapter Five: Physical Security of the White House

Chapter Six: Physical Security of the Executive Office Building

Chapter Seven: Personnel Security Clearances

~~TOP SECRET~~

~~TOP SECRET~~

April 30, 1965

SURVEY OF TECHNICAL AND PHYSICAL SECURITY PROTECTION
FOR THE PRESIDENCY

I. INTRODUCTION - THE PROBLEM

Basic Factors and Premises

Factors which underlie the conclusions and recommendations of this survey are as follows:

- The volume of concentrated, authoritative information bearing on the full range of U. S. national and international concerns which pass to, from, and within it each day makes the White House a prime intelligence target. The increasingly centralized direction of foreign affairs and the growing amount of information communicated electronically will increase the attractiveness of this target in the future.

- Motivations to tap these information sources are very high. As one consultant to this study observed, "We simply have not recognized temperamentally the efforts which our adversaries are willing to expend in this field." The thirst for intelligence (and news) is particularly high in crisis periods when the speed and intensity of action tends to reduce the security of the information process.

- There has been a marked and continuing expansion in technical capabilities for clandestine eavesdropping available to intelligence agencies and also to news, business, and political groups. Domestically,

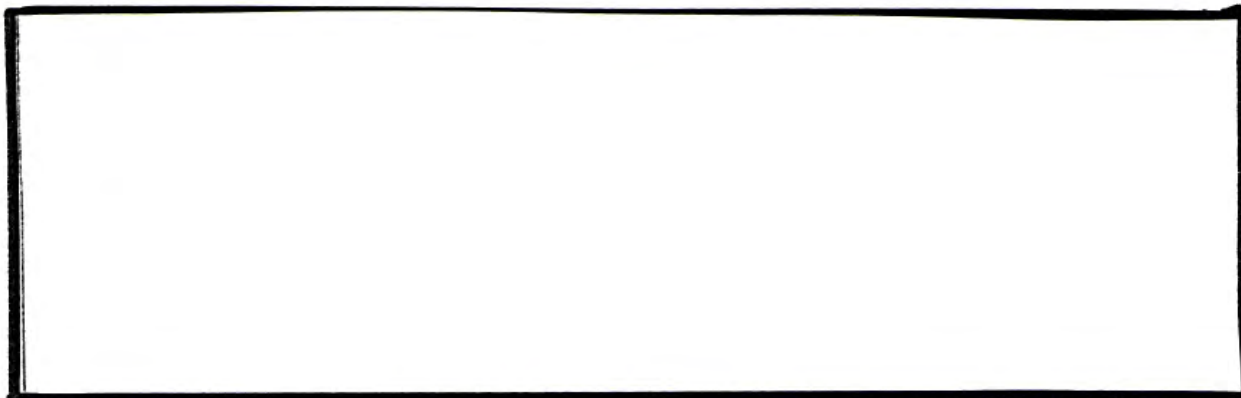
~~TOP SECRET~~

eavesdropping devices are available on the commercial market, and a growing number of private detective agencies stand ready to provide eavesdropping services. Overseas, the Soviets and other Bloc powers have demonstrated high proficiency and activity in this area, as evidenced in the operations against the U. S. Embassy in Moscow since 1952, and some 750 audio surveillance devices found to be targeted against U. S. and allied facilities abroad since 1949. No devices of foreign origin have been found in the U. S. itself.

- In the next five years, intensive application of microelectronics and other developments now in the laboratories will increase significantly (a) the use of clandestine surveillance systems, and (b) the difficulty in countering them effectively.

- Given the importance of the office and the motivations and capabilities of potential penetrators, added precautions should be taken to protect the President's privacy and security, using the best personnel, techniques, and equipment available. The payoff from such an effort in terms of national security and protection of the institution of the President would appear to be many, many times the small cost involved.

Pages 3 and 4 sanitized in entirety.



Objectives and Approach of the Survey

This survey, in response to National Security Action Memorandum 315, has the following general objectives:

- To assess for the President and his advisers the risks of compromise involved in the use of various communications and other facilities.
- To assess the present program for protecting the privacy and security of the Presidency given the present capabilities for technical penetration.
- To assess the handling of classified documents in the White House, especially certain highly sensitive documents sent to the President.
- To recommend specific measures to reduce risks, which are realistic in terms of cost and the needs and functions of the White House.
- To recommend a sound and continuing technical protection program which would minimize the possibilities of compromise or embarrassment to the Presidency.

To conduct the survey, the Director of the Bureau of the Budget convened a committee of experts from CIA, NSA, State, and Defense, and representatives of the Executive Office (Attachment A of the Summary Report), hereafter referred to as the Steering Group. In addition, the survey approach and the conclusions have been reviewed by a panel of scientific and engineering consultants consisting of Dr. Jerome B. Wiesner, Dr. William O. Baker, Dr. Edward David, and Mr. Richard James (see Attachment A). The conclusions are based upon results of inspections and extensive discussions with appropriate representatives of the White House, Secret Service, FBI, CIA, Defense, and other agencies, and the telephone companies (AT&T, Chesapeake and Potomac, and Southwestern Bell).

In the course of the survey, it was determined that conditions in two areas required more detailed and comprehensive inspections, and these were initiated:

- Defense investigated possible compromising radiations from equipment utilized for secure or encrypted communications. A team of Army specialists, supported by NSA, conducted this inspection, known as TEMPEST. (See Chapter Three.)
- Secret Service, augmented by equipment and highly trained personnel from State, Defense, and CIA, conducted an intensive audio countermeasures survey of the White House. This work is still in progress.

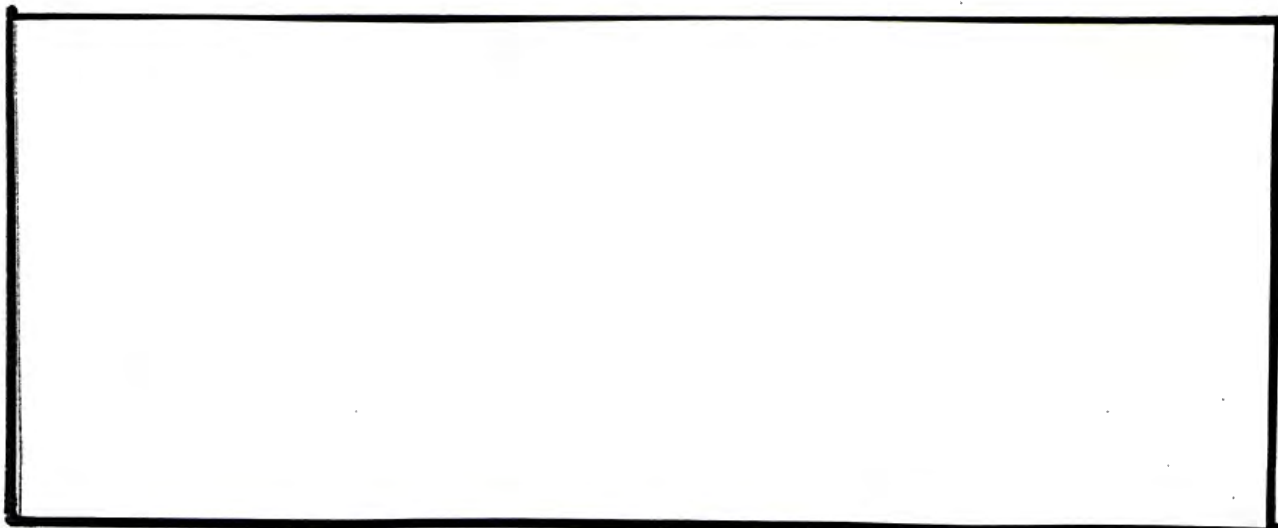
~~TOP SECRET~~

7

This report concentrates on security protection at the White House but also touches upon relevant situations at the President's ranch in Texas, at the office in Austin, Texas, and while he is travelling. The problems of the Executive Office Building (EOB) and, to a lesser extent, the new Federal Office Building No. 7 are treated as they related to White House problems, primarily in the area of communications.

Two panels dealt with special aspects of the problem. The first panel, chaired by [REDACTED] CIA, assessed audio countermeasures and related physical and personnel security. The second, chaired by Leo Rosen of NSA, assessed communications security. The chapters which follow the Summary Report contain the detailed findings and recommendations of the two panels.

II. ASSESSMENT OF RISKS AND VULNERABILITIES



~~TOP SECRET~~

On several occasions, questions have been raised as to the relationship between audible clicks on telephone lines and possible tapping. Based upon a study by the Chesapeake and Potomac Telephone Company, the greatest source of clicks is the operator checking the line to see if calls are completed. Clicks also result from maintenance people checking lines and very infrequently from natural phenomena. A hostile telephone tap generally cannot be detected audibly.

The findings of the survey as to major vulnerabilities of the White House information processes are as follows (generally ranked from most to least vulnerable):

1. Most vulnerable are mobile radio telephones in cars, helicopters, and aircraft. It must be assumed that the Soviets monitor all radio telephones in the Washington area from their Embassy. The Presidential aircraft would also be a prime monitoring target, and the Steering Group has seen transcripts of classified conversations from the aircraft to the White House recorded by an Air Force contractor, Radio Liberty, in Iowa. Similarly, the "IBJ network" in Texas can be monitored by anyone within range with simple radio equipment.

2. Private line telephone service from the White House switchboards to residences and offices can be monitored in the normal course of business by operators at the White House switchboards and by maintenance men and operators at the telephone exchanges (usually two or three exchanges)

where the lines are tagged for special service. The lines to residences are vulnerable to tapping near the residences where they become easily identified (they usually follow the same routing as normal telephone service).

As an example of the vulnerability of private line service, Secretary McNamara's private line was found to run along the back wall of the Finnish Embassy. A Finnish employee of the Embassy stated casually to a member of the survey team and a telephone company employee, "Mr. McNamara has his lines in this cable; we listen to him all the time." This service has since been rerouted.

Secretary Rusk's two private White House lines "appear" eight times in terminal boxes where they are easily accessible to maintenance and to tap. A potential tapping operation would be masked by the wooded area through which the service passes. One of the line appearances was on the property of a registered agent of the Dominican Republic.

In the physical survey of private line service near the residences of 12 key advisers to the President, it was apparent that a potential tapper would have easy access to essential poles, cables, and terminal boxes. On two occasions when people were encountered, the statement, "We're with the telephone company," satisfied curiosity and stopped further questioning. In reviewing Secretary McNamara's terminals in his basement, survey members were admitted without question and spent about five minutes unescorted examining the terminal (see Chapter Two, page 22).

3. Long distance telephone service to and from the LBJ ranch is highly vulnerable to intercept in the open wire carrier and microwave links between the LBJ ranch and Austin. The microwave, particularly, can be monitored at a distance with a radio receiver with little chance of detection.

4. Clear text of classified messages was recovered by reading emanations from secure teletype equipment at the LBJ ranch on the open wire power lines from the ranch house for a distance of 3/4 mile. Recovery of the same information was made from the telephone lines and microwave system going from the ranch to Austin (since corrected).

5. The secure teletypewriter equipments in the White House communications center and the International Situation Room also were found to be high-level "radiators," which, in conjunction with improper intermixture of secure and non-secure telephone lines, provided potential paths for transmission of clear text information of encrypted messages out of the White House.

6. The counter audio survey has found numerous places where there is accoustical leakage from sensitive offices. Conversations in Mr. Moyers' office could be heard through the wall into a press area and through an old sink pipe down into the dispensary below. Similarly, an unused pipe conveys intelligible sound from the Cabinet Room to a Secret Service squad room below.

7. Given the number of people moving in and out of sensitive spaces, the introduction of a small, self-powered radio transmitter which can be quickly concealed by people having limited access (workmen, TV technicians, char forces) presents a possible form of technical penetration. The miniature recorder (cigarette package size) which could be easily concealed also presents a threat.

8. There are direct, live audio lines from the Cabinet Room to television and radio networks. Such lines also appear in the hall outside the President's office. The potential of a quick connection of a microphone to one of these lines constitutes a hazard.

9. Telephone service for the Executive Office Building (EOB) is more vulnerable to intercept than that in the White House. First, it is served from a terminal room in the basement where wiring conditions, and hence the ability to spot cross-connections, are exceptionally poor. Second, the building was completely open to the public during office hours up to about three years ago, and it is still susceptible to unauthorized entrance and free movement within it. Third, the service goes through the Lafayette exchange where it can be monitored by GSA operators. It should be noted that the White House lines to the offices of Secretaries Rusk, McNamara, Fowler, and Udall pass through the EOB basement terminal room and that most of the NSC staff supporting Mr. Bundy (all when the study began) are served through this room and the Lafayette exchange.

10. Presidential telephones could be cross-connected or tapped in two terminal points in the White House where his service is intermixed with other telephone service (press, TV, radio, Muzak) going directly out of the White House, not through the manual switchboards. Wiring conditions in these rooms were such that it would be extremely difficult to identify an improper cross-connection or tap. In addition, all Presidential calls through the White House switchboard are accessible in the EOB at a terminal where there is an intermixture of service and much excess equipment and cabling as well as at the switchboard itself (see Chapter Two, page 7 ff.).

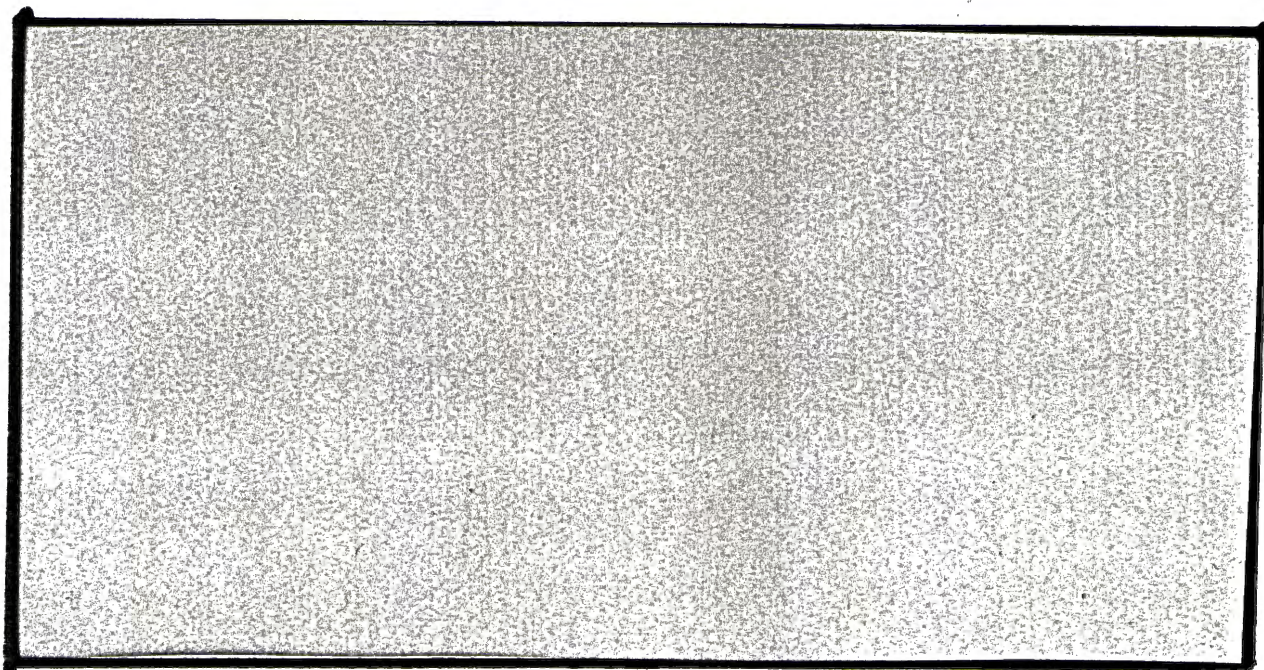
11. In the survey, a safe containing Top Secret material was observed, left open overnight. More significant, perhaps, this particular safe (and one other found later) still had the basic combination (50-25-50), which had been on it since the safe was delivered from the factory. Classified documents left out overnight were frequently observed.

12. Use of wired microphones, carrier transmitters, or compromised "hot" telephones present substantial problems of transmission in and out of the White House, but should not be ruled out given present wiring conditions. Extensive access to telephone and electrical systems would be required.

13. The three underground "feeder" telephone cables from the White House to the downtown and mid-town exchanges and more particularly the

100 pair cable to the mid-town exchange offer relatively attractive possibilities for tapping which are made easier by tagging all White House lines in the exchanges to ensure good service. Tapping of the cables themselves in a little used manhole or by means of a tunnel into the cable vault would be more difficult.

14. Sophisticated penetration techniques such as infra-red windowpane pickoff, laser beams, lip reading by telescope, directional parabolic microphones, etc., appear to be limited by physical conditions at the White House and the state of the art. However, advanced developments in some of these areas must be carefully watched and considered in developing future protection programs.



No defensive system will provide 100 percent protection against clandestine eavesdropping. However, substantial security improvements can be made without disruption of the White House work processes and without significantly altering the symbolic openness and approachability of the Presidential office.

III. MAJOR CONCLUSIONS AND RECOMMENDATIONS WITH RESPECT TO GENERAL SECURITY AND AUDIO SURVEILLANCE COUNTERMEASURES

Overall Security Responsibility

In marked contrast to the need to protect the security and privacy of the President, there is actually no coherent security program at the White House, and little indication that one is being developed. No one is in charge to direct the fragmented security functions. Security files for White House personnel are reviewed by Mr. Watson; Mr. Moyers has responsibilities for approving White House pass issuance; Mr. Bundy controls the handling of most classified documents; Secret Service with the White House police provides certain physical security; Secret Service exercises responsibility for audio countermeasures for most of the White House and security pertaining to administrative (non-military) communications; the White House Communications Agency (WHCA) provides security for its communications; and the FBI performs full field investigations and specific counter audio and communications investigations on call.

This diffusion of responsibility has resulted in wide gaps in White House security. It certainly is not conducive to developing a program to meet the increasing technical threat.

It is recommended that:

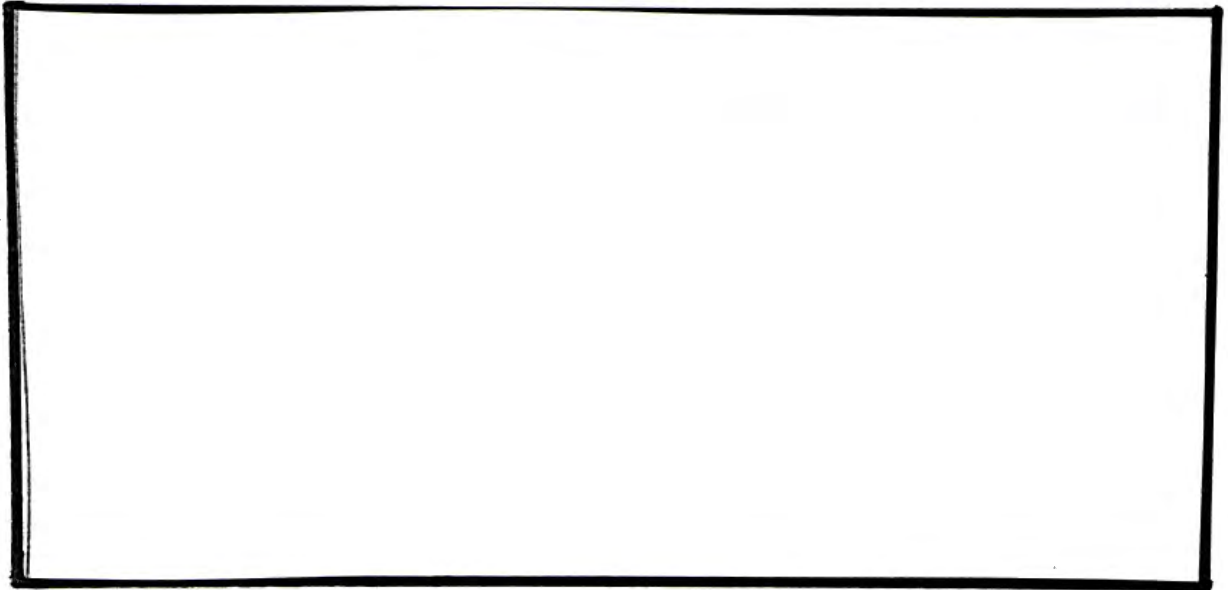
1. Responsibility for physical security, telephone security, audio countermeasures, and personnel clearances should be clearly assigned to a single Presidential assistant. With proper staff support as recommended, the security assignment would take only a small portion of the assistant's time.
2. Staff support for the designated Presidential assistant should be provided by a professional, high-grade security officer reporting directly to such assistant and responsible for ensuring that a comprehensive security program is established and maintained. The security officer should have broad experience in the several areas of security and should have a small staff.

Audio Countermeasures Program

The Secret Service program to protect the President from technical eavesdropping began in the early phases of World War II. Protection of Presidential privacy was assumed to be a logical extension of the statutory responsibility "to protect the person of the President" and his immediate family. Yet, as late as 1962, there were only two people concerned with audio countermeasures. In the last year, the number has been increased to six, although only about 50 percent of their time is spent specifically on audio countermeasures.

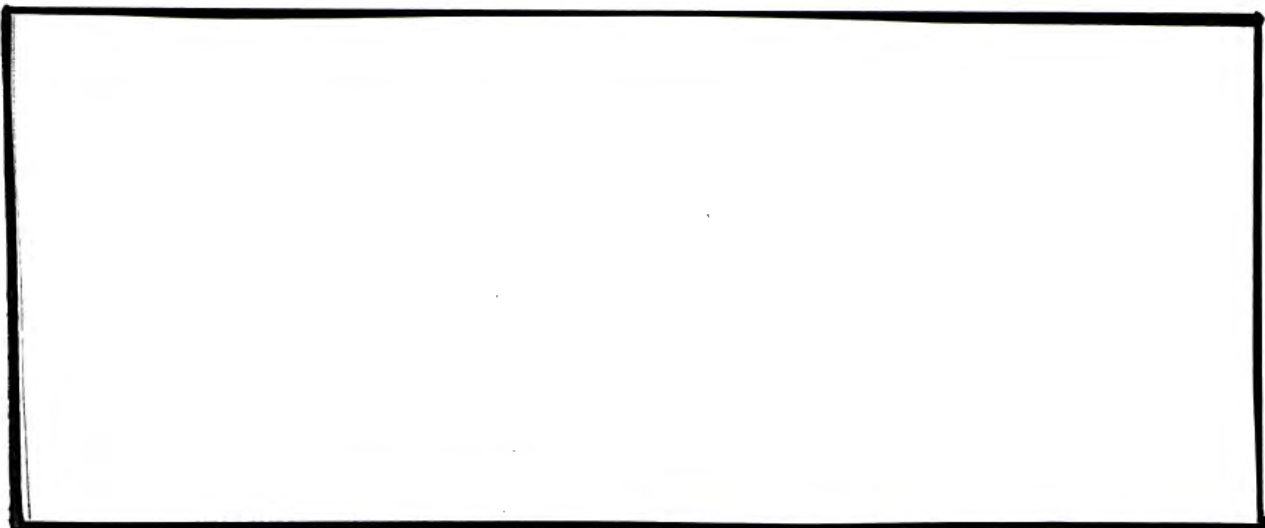
However, to this day, there is no statutory authority or written directive assigning Secret Service any responsibility for audio countermeasures.

Also, there has been no guidance or direction from outside the Secret Service (either the White House or the Treasury) indicating the degree of emphasis to be given to this function. It is not surprising that the Secret Service, oriented largely to protective and investigative functions, has not allocated enough of its scarce budgetary and manpower resources to the countermeasures effort. The program has tended to drift along with the following results:



Chapter One contains a detailed review of the program and 16 specific recommendations for improvement.

There are good reasons for having the Secret Service provide "in-house" audio surveillance countermeasures capability as many of these functions



We conclude that the Secret Service can and should develop an effective countermeasures program, if the recommendations herein for strengthening its capabilities in this field are implemented. The alternatives -- assigning responsibility for this function (a) to WHCA, (b) to a new civil service unit attached to the White House or some office in the Executive Office of the President, or (c) to an operating agency like State, Defense, or CIA -- were considered and rejected as less desirable. If it appears, however, that after a year the Secret Service program has not developed the technical leadership and competence required, alternative arrangements should be reconsidered.

It is recommended that:

3. Responsibility for the audio countermeasures program in the White House (including the East Wing Shelter and residences of the Vice-President and key Presidential staff) should be clearly assigned to the Secret Service by Presidential memo-

randum, and execution should be under the direction and guidance of the proposed White House Security Officer. The Secret Service should also be responsible for surveillance of buildings around the White House which might be used as possible listening posts.

4. Efforts should be made to obtain a highly qualified technical director for the countermeasures program. If Secret Service is not able to hire such a person, he should be detailed for periods of two - three years from an agency in the intelligence community having substantial technical programs.

5. Within Secret Service, the technical security function should be separated from the Protective Research Section and given greater organizational emphasis.

6. The frequency and coverage of the audio countermeasures program should be increased as recommended in Chapter One, and at least five people added to the present staff of six. All staff should be technically trained, and at least half should be graduate engineers.

7. The White House Security Officer should be a permanent member of the Technical Surveillance Countermeasures Committee of the U. S. Intelligence Board in order to keep abreast of developments and to obtain advice and assistance as needed. The technical director of the Secret Service countermeasures program should attend meetings of the Research and Development and Audio Countermeasures Sub-Committees.

8. The Secret Service countermeasures program should be reviewed in a year by a committee created by the Director, Office of Science and Technology, to ensure that progress is being made toward developing an effective program in terms of the threat. The Director should make recommendations to the President through the designated Presidential assistant for security.

Security Aspects of Construction and Repair Activities

Many people in the White House initiate changes in telephones and physical arrangements on a rush basis with little consideration given to security. These changes may be implemented by the White House Communications Agency (WHCA), the telephone company, GSA, the National Park Service, the Navy, or some other agency, and no one person has a complete picture of what is being done or about to be done. It is not an infrequent occurrence that Secret Service first hears of a project in the daily notice that contractor employees will arrive on the job. Once features are installed, it is more costly (and sometimes infeasible) to make changes which might be required for security reasons.

It is recommended that:

9. Regular procedures be established for coordinating physical changes in advance with the proposed Security Officer, especially all changes in telephones and electrical systems.

Personnel Clearances and Control of People

In the last few months, clearer and more effective procedures for reviewing FBI investigations and approving assignments to the White House staff and military personnel have been established. However, there are still somewhat diffused authorities for conducting investigations, reviewing reports, and issuing passes for maintenance people, vendors, and tradesmen. The system is not geared to the need to protect against technical penetration. For example, the 60 telephone maintenance men permanently assigned to the White House, who have access to vital telephone systems, do not receive the FBI full-field investigations given to regular White House employees, including cooks and gardeners.

Control of workmen within the White House, from the viewpoint of preventing penetrations, is haphazard. Permanently assigned telephone people have White House passes and free run of the facility, except for the President's office. When, for particular rush jobs, additional telephone people are brought in they are placed under the supervision of the 60 regular pass holders for most areas. GSA electricians and maintenance people with passes are treated similarly. Other workmen with visitor badges are generally escorted, often rather loosely, by a White House policeman who has not been trained in identifying technical penetrations, and whose main objective is to see that the men do not wander off toward the President. The Steering Group has observed cases where the "escorting"

officer sat in the hall watching a door from the outside, while workmen operated freely and unobserved in sensitive offices.

It is recommended that:

10. The proposed Security Officer be given authority to establish and maintain appropriate and consistent security standards for investigation and review of all persons having duties in the White House or access to it.

11. Authority for granting clearances and issuance of White House passes should rest with the proposed Security Officer under the supervision of the designated Presidential special assistant for security.

12. All people permanently assigned to the White House, including telephone company and GSA maintenance personnel, should be given full field FBI investigations (except Secret Service, White House police, and military personnel who are investigated otherwise).

13. All workmen who have prolonged access to the electrical or telephone systems serving sensitive areas, who have not been given full FBI investigation, should be escorted by technically trained members of the Secret Service countermeasures unit.

Classified Document Handling

The survey was concerned with the security of procedures for handling classified material in the White House and the LBJ ranch. The survey did not deal with the efficiency of this process or with the handling of unclassified documents.

By far, the larger percentage of total volume of written material received and handled within the White House is unclassified, although much of it is sensitive. As a general rule, White House personnel appear to operate on the premise that all papers addressed to the President are automatically "Confidential" and "Personal" in nature, and this general approach undergirds the system for handling formally classified documents.

The survey revealed that there are no written procedures now in effect for controlling and moving or for storing classified documents in the White House. However, with respect to the control and movement of such documents, a less formal system has evolved, centered primarily on Mr. Bundy's operation, which appears effective considering the unique situation of the White House, the pace at which papers are handled, and the lack of any overall security authority noted above. Although the committee was informed of lapses which have occurred in the past, the people with whom the problem was discussed exhibited a reasonable and consistent understanding of the control system.

The storage of classified documents is a different matter. The Steering Group was advised that responsibility for securing classified documents at the close of the day resides in each office. However, the Group observed enough instances of Top Secret papers being left on desks at night to conclude that this is a common occurrence. The physical protection program provided by the White House police does not appear to warrant this confidence, especially given the number of loosely escorted workmen and char force personnel wandering around the White House after hours.

With respect to assignment of responsibilities, it is clear that the President's Assistant for National Security Affairs will, by the very nature of his task, have to handle the vast majority of classified documents, especially those involving special categories of clearances. It was indicated that about 95 percent of classified documents flow through the Bundy complex. It, thus, makes sense to concentrate the handling of such paper in his office, backed by the NSC staff as is now the case. However, overall responsibility for ensuring that there is a system, that it fits adequately with the rest of the physical security program, and that it is adequately understood, especially by secretaries and administrative assistants in all offices, should be exercised by the proposed White House Security Officer.

We have reviewed with special care the handling of the highly classified material which becomes a part of the President's "night reading" file, particularly the State Department's "Evening Reading" and CIA's "President's Daily Brief," the latter containing COMINT and other highly sensitive material. It is concluded that, although these materials appear to be handled with awareness by all concerned, the security of the process would be improved by reducing the number of people who handle or have access to these materials on the way to the President. For example, these materials, generally received in Mr. Bundy's office between 6:30 and 7:00 P.M. each evening, are forwarded to the President's secretary for inclusion in the night reading file, delivered by a White House messenger to the Head Usher, handed to the Doorman, who either gives them to the Sergeant valets on duty or takes them directly to the President's private quarters. If the President is out for the evening, the documents remain untended on his bed until his return to the White House.

It is recommended that:

14. The proposed Security Officer should establish policies and procedures for the handling and storage of classified material in the White House. White House secretaries and administrative assistants should be thoroughly briefed on these procedures (and other aspects of the security system).

15. Highly classified documents for the President's night reading should be held in the Situation Room when the President is out for the evening and should be delivered to the President's quarters by the Watch Officer when notified of the President's return.

16. The procedures for checking and locking up classified documents at night should be reviewed by the Security Officer and strengthened. The role of Secret Service and White House police in this process should be clarified.

Other Technical and Physical Security Measures

Much remains to be done after this survey is completed. For example, the proposed Security Officer should be responsible for initiating:

- A comprehensive program to map sensitive spaces of the White House accoustically and electrically.
- A systematic program to identify and remove if not in use all telephone, electrical, and other wire in the White House.
- A "base" physical security survey of the White House (starting with the information developed in this survey).

IV. MAJOR CONCLUSIONS AND RECOMMENDATIONS
WITH RESPECT TO TELEPHONES AND COMMUNICATIONS

Basic Findings

The telephone security problem at the White House is inherent in the system. The present telephone system in the White House grew like Topsy and certainly was not designed with security in mind. There are (a) too many switchboards with too many operators who can overhear conversations, (b) too many terminal boards where cables from sensitive telephones intermix with service going directly out of the building (e.g., to the news media), and (c) too much excess wiring and equipment lying available for use in possible technical penetrations. System records are inadequate, and no one knows the whole system.

The outside commercial telephone systems serving the White House (and the ranch in Texas) were built with reliability and economy as primary objectives. These systems are basically insecure and vulnerable at many points to the determined and trained tapper. There is no practical way to make the telephone service outside the White House effectively secure, unless crypto-secure telephones are used. However, recommendations made in this report will help to reduce risks somewhat.

Need for Overall Responsibility

As in the general security area, there has been no clear responsibility for planning communications in the White House, particularly technical

planning. It is believed that communications are so important to the President that general responsibility should be placed in one Presidential assistant. This assistant, however, must be given strong technical support.

The most logical official to provide such technical support is the Director of Telecommunications Management (DTM), who already performs a number of communications functions for the President, including the development of Presidential requirements for inclusion in technical planning for the National Communications System (NCS). With a small staff of competent engineers, the DTM could work with the telephone companies, WHCA, the Defense Communications Agency, and others to see that longer term system capabilities provided the President are modern, secure, and adequate to his informational and command needs. In planning the security features, the DTM should work closely with the proposed Security Officer and technical director of the countermeasures program.

It is recommended that:

1. Responsibility for Presidential communications should be placed clearly on a single Presidential assistant, preferably the same person having general security responsibility.
2. On technical matters, such as the planning of facilities and capabilities, including security features, the designated

special assistant should look to the DTM for support. The DTM should acquire the necessary technical competence to perform this task.

Planning for a New, More Secure System

WHCA's "Signal" switchboard has already reached its capacity, and the White House switchboard at the present rate of growth in service is expected to reach saturation next year. Ever since the White House board was moved to the EOB in 1962, the system has been considered an "interim" arrangement by the Chesapeake and Potomac Telephone Company.

The President needs an effectively planned communications system with the best features of privacy and security built into it from the beginning. Basic questions with respect to a new system are (a) whether it should be self-contained (electronically segregated and physically secured), and (b) how much of the Executive Office of the President it should embrace. With respect to the latter, the long-run trend will be to move more activities directly supporting the White House into the EOB and Federal Office Building (FOB) No. 7. It would appear prudent in telephone planning at this time to consider the White House - EOB - FOB No. 7 as a single complex served from a central switchboard in the EOB. This switchboard could have dual capabilities -- (a) manual capability serving the President and top staff as determined by later studies, and (b) a flexible, rapid dial system which could ring anyone in the complex by dialing only two or three digits.

This single system should largely replace the three switchboards now in use with considerable savings in the number of operators, trunking, and line costs. In fact, the C&P Telephone Company has estimated that such new service could be rendered for approximately the same annual recurring cost as that for the present system. In the system studies which are required, these cost factors should be carefully weighed.

It is recommended that:

3. The designated Presidential assistant for communications should request the DIM to work with the telephone company, WHCA, Defense, GSA, and the White House Chief Clerk to develop and to recommend a rational telephone system for the White House - EOB complex, with consideration of the following security features:

a. A self-contained system serving the whole White House - EOB complex.

b. A combination of manual operation and a flexible dial system so that calls can be made without going through the operator.

c. An automatic disconnect capability, even for the dial portion, so that when the inside telephone is hung up, the line into the White House does not remain open to outsiders.

d. Some form of operator disconnect on calls that have been established so that the operator cannot re-enter the circuit except on recall by the parties.

- e. Maximum cryptographic security for links outside the complex.

Crypto-Secure Telephones

The only way that telephone calls outside the White House compound can be completely protected is through use of crypto-secure voice systems.

Marked improvements in quality are being made, and the new KY-3 telephone is equal in quality to that of regular telephones. These should be installed at vital White House links as soon as feasible (KY-3 facilities now exist from Mr. Bundy's office to the Secretary of State and to the ranch).

However, the new secure voice service should not be made available to the President until it has been proven elsewhere and will clearly meet his needs. There has been a tendency in the past to use the White House as a proving ground for completely new communication equipment, before the functioning and security of the equipment have been established.

The present proposal to install a secure facsimile capability between the Pentagon and the Situation Room appears to be an example. The security characteristics of this equipment should be thoroughly demonstrated before installation.

It is recommended that:

4. KY-3 high-quality, secure telephones be installed, as soon as feasible in circuits between the President and offices and residences of key national security advisers. Secure voice capabilities for Presidential aircraft, helicopters, and cars should be developed and installed when ready. The critical point is the acceptance and use of these telephones once installed.

Responsibility for Telephone Security at the White House

For historical and practical reasons, there is a split responsibility for providing regular, non-secure telephone service at the White House, and this split complicates the fixing of responsibility for telephone security. The White House board, manned by civilian operators under the direction of the White House Clerk handles the majority of incoming and outgoing traffic. WHCA handles the balance through the Signal Board. WHCA also has operational responsibilities for crypto-secure communications at the White House and for all communications at the IBJ ranch and while the President is travelling. The local telephone company installs and maintains most of the equipment used by both services.

Secret Service has exercised some responsibility for the security of telephone service running through the White House board. However, the Steering Group was told that until 1959 the telephone company kept terminal rooms in the White House locked and did not allow Secret Service

inspection. Since that time, the company has made system information available to the Secret Service, but not enough to permit a thorough assessment of security.

Since a major portion of the telephone security is encompassed in a strong audio countermeasures program, we believe that the Secret Service should assume responsibility for security of all non-crypto-secure telephones. WHCA should continue its responsibilities in the area of crypto-secure telephones. However, this division may need to be reviewed in the future if there is a move toward a combined switchboard in the EOB and if more crypto-secure voice service is introduced into White House offices.

It is recommended that:

5. Under the guidance and supervision of the proposed White House Security Officer, the Secret Service should, as a part of its audio countermeasures activities, be responsible for protection of all White House telephones (including those operated by WHCA) which are not cryptographically secure.

6. The designated special assistant for communications be the focal point for guidance to WHCA. With technical support from the DTM, he should review the relationship between WHCA and other elements providing regular telephone service at the White House.

Other Telephone Recommendations

7. Until secure phones are available, the Secret Service should check the private line service to key residences of White House officials through the exchanges and from the last exchange to the residence in order to identify and to have corrected obviously insecure conditions.

8. Key staff of NSC supporting Mr. Bundy should be served by the White House board, rather than through existing FOB terminals and the downtown exchange.

9. The speaker phones being used by the President and his immediate staff should be tested to be sure they are not radiating information out of the White House (NSA has initiated such tests.) Steps should be taken to see that the "live" audio from these speaker phones is carefully confined electrically.

10. The WHCA recording studio should be moved away from the President's office.

11. NSA, with assistance from the Bell System, should explore the feasibility and cost of providing an appropriate number of secured circuits for the vulnerable LBJ ranch - Austin link and to make recommendations to the special assistant designated for communications.

Compromising Radiations (TEMPEST)

The encrypted communications at the White House Communications Center in the East Wing, as found by the survey, had been installed by WHCA at a time when little attention was paid to the problem of compromising radiations. What is more, WHCA had not requested a TEMPEST check for such radiations since 1962, although standing procedures called for inspections at least every year. The preliminary survey of the WHCA communications area in the East Wing Shelter showed a number of unacceptable practices, including the use of a high-level teletypewriter cryptographic equipments which under previous tests have been proved to produce compromising emanations. Corrections have since been made, and a TEMPEST check has been completed.

Similar conditions were found in the International Situation Room.

However, the potential pick-up of these radiations is considered more dangerous, because the Situation Room is at ground level on West Executive Avenue. TV trucks and other vehicles parked in the area pose a potential threat. These problems still await correction, after which a TEMPEST check should be made.

The situation in the WHCA communications trailer at the IBJ ranch was basically the same as that at the White House - i.e., the cryptographic equipment was programmed for high-level signal operation. Readable signals were obtained by Army technicians near the overhead power line

three quarters of a mile from the ranch. Clear text radiations from classified messages being sent or received at the ranch were thus getting into both the open wire telephone carrier and microwave system to Austin. These conditions have been corrected.

It is recommended that:

12. The WHCA facilities be regularly inspected to ensure continued compliance with TEMPEST standards, and these tests should be supported by NSA.

13. WHCA personnel should receive continuing technical guidance from Army Security Agency, NSA, and others to keep abreast of advances in the TEMPEST and communications security field.

14. Prior to any additional secure communications systems or equipment being installed, including the proposed secure television and facsimile systems, detailed plans should be prepared and concurred in by a TEMPEST-trained staff.

15. Steps should be initiated to reduce radiation levels from "soft talk" teletypewriter equipment used with Presidential aircraft.

White House Office Machines

The survey group attempted to identify automatic office equipment which might radiate recoverable intelligence. On inspection, it was determined

that the Xerox machines used for classified information in the White House and the EOB constitute no risk. However, the two Flexowriters, two Royaltypers and four Robotypers used in room 59 of the EOB under the administrative control of the White House do represent a potential hazard.

It is recommended that:

16. Controls should be placed on the above-mentioned machines in room 59 to ensure they are used only for unclassified or, at most, Confidential information.

17. If, in the future, any office machines are installed, particularly if this is electronic data processing equipment, consideration should be given to the resulting possibility of compromising radiations.

*Do appendices
carry any new stuff
let the document show this*

*M-5B/65-2/12 C.2
Gordon Chase*

DRAFT
4/23/65

3

SURVEY OF TECHNICAL AND PHYSICAL SECURITY ARRANGEMENTS

FOR THE PRESIDENCY

I. OBJECTIVES AND APPROACH OF THE SURVEY

The survey, in response to National Security Action Memorandum 315, has the following general objectives:

- To assess for the President and his advisers the risks of compromise involved in the use of various communications and other facilities
- To assess the present program for protecting the privacy and security of the Presidency in terms of current capabilities for technical penetration.
- To recommend specific measures to reduce risks, which are realistic in terms of cost and the needs and functions of the White House.
- To recommend arrangements for a sound and continuing technical protection program paced to the growing risks which would minimize the possibilities of compromise or embarrassment to the Presidency.
- To assess the handling of classified documents in the White House, especially certain highly sensitive documents sent to the President

To conduct the survey, the Director of the Bureau of the Budget convened a special committee of officials from CIA, NSA, State, and Defense, and representatives of the Executive Office (listed on Attachment A), hereafter referred to as the Steering Group. These men were selected to provide a balanced expertise in intelligence and security from both an operational and research and development viewpoint. In addition, the survey and the

SANITIZED

E.O. 13526, Sec. 3.5

NLJ/RAC 05-47

By *isl* NARA, Date 12-6-11

~~SECRET~~

2

conclusions have been reviewed by a panel of scientific and engineering consultants consisting of Dr. Jerome B. Wiesner, Dr. William O. Baker, Dr. Edward David, and Mr. Richard James (see Attachment A). The conclusions are based upon results of inspections and extensive discussions with appropriate representatives of the White House, Secret Service, FBI, CIA, Defense, and other agencies, and the telephone companies (AT&T, Chesapeake and Potomac, and Southwestern Bell).

In the course of the survey, it was determined that conditions in two areas required more detailed and comprehensive inspections, and these were initiated:

- Defense investigated possible compromising radiations from equipment utilized for secure or encrypted communications. A team of Army specialists, supported by NSA, conducted this inspection, known as TEMPEST (see Chapter III).
- Secret Service, augmented by equipment and highly trained personnel from State, Defense, and CIA, conducted an intensive audio counter-measures survey of the White House. This work is still in progress.

This report concentrates on security protection at the White House but also touches upon relevant situations at the President's ranch in Texas, at the office in Austin, Texas, and while he is travelling. The problems of the Executive Office Building (EOB) and, to a lesser extent, the new Federal Office Building No. 7 are treated as they related to White House problems, primarily in the area of communications.

~~SECRET~~

~~SECRET~~

3

The detailed aspects of the survey were treated under two headings. A panel, chaired by [REDACTED] CIA, assessed the audio counter-measures and related physical and personnel security aspects of the problem. A second panel, chaired by Leo Rosen of NSA, focused on various aspects of communications security. The chapters which follow the Summary Report contain the detailed findings and recommendations of the two panels.

Who
came?

The conduct of the study was delayed initially by the lack of basic information on the White House telephone system on which to base an assessment. This information was provided on March 1, 1965. Also the fact that there is no central authority on security procedures at the White House meant that it was necessary to obtain information from a number of sources, and such information often proved conflicting.

Where possible in the course of the study, changes which might improve security were suggested and accomplished. Examples of changes already made or being made are:

Who
came?
This would
interest

Put
the changes

~~SECRET~~

4

1. Fundamental reductions have been made in possible compromising radiations from communications equipment handling classified material at the White House and the LBJ ranch.

2. Steps have been taken to design and fabricate transportable cryptographic communications equipment with reduced radiation levels which could accompany the President on trips, particularly abroad.

3. The ^{C&P} telephone company in connection with certain new installations is installing shield cables direct from telephones in the West Wing to a consolidated terminal room now under construction.

4. White House Police are now being taken to State for briefings in the audio surveillance threat and countermeasures.

5. The Secret Service has installed alarms in telephone terminal areas and other sensitive areas.

6. A better understanding of the technical penetration problems in the telephone companies has come about through very helpful discussions with representatives of AT&T, Chesapeake and Potomac, and Southwestern Bell, and these companies are considering development of technical features which would increase telephone security and privacy.

7. About 3,000 feet of surplus cable not needed for present service has been removed in the course of the special counter audio survey.

Sections II and III of the Summary Report which follow set forth basic findings and premises of the survey and assess the potential vulnerabilities of various Presidential facilities, concentrating on the White House. Major conclusions and recommendations are summarized in two separate but interrelated sections: IV. General Security and Audio Surveillance Countermeasures; and V. Telephones and Communications.

II. BASIC FINDINGS AND PREMISES OF THE SURVEY

Findings and premises which underlie the conclusions and recommendations of this survey are as follows:

1 - The White House is a prime intelligence target, because of the volume of concentrated, authoritative information bearing on the full range of U. S. national and international concerns which pass to, from, and within it each day. A rapidly growing amount of this information is passed electronically.

2 - Motivations to tap these information sources are very high. As one consultant to this study observed, "We simply have not recognized temperamentally the efforts which our adversaries are willing to expend in this field. // The thirst for intelligence (and news) is particularly high in crisis periods when the speed and intensity of action tends to reduce the security of the information process.

3 - There has been a marked and continuing expansion in technical capabilities for clandestine eavesdropping available to intelligence agencies and also to news, business, and political groups. The Soviets and other Bloc powers have demonstrated high proficiency and activity in this area, as evidenced in the operations against the U. S. Embassy in Moscow since 1952, and some 350 audio surveillance devices found to be targeted against U. S. ^{and other} facilities abroad since 1949. Domestically, eavesdropping devices are available on the commercial market, and a growing number of private detective agencies stand ready to provide eavesdropping services.

~~SECRET~~

7

④ - In the next five years, intensive application of microelectronics and other developments now in the laboratories will increase significantly (a) the use of clandestine surveillance systems, and (b) the difficulty in countering them effectively.

④ - Given the importance of the office and the motivations and capabilities of potential penetrators, extraordinary precautions should be taken to protect the President's privacy and security, using the best personnel, techniques, and equipment available. The payoff from such an effort in terms of national security and protection of the institution of the President would appear to be many, many times the small cost involved.

④ - It is believed that security improvements recommended herein can be made without disruption of the White House work processes and without significantly altering the symbolic qualities of openness and approachability of the Presidential office.

~~SECRET~~

~~SECRET~~

III. ASSESSMENT OF RISKS AND VULNERABILITIES

Basic conditions at the White House

From the point of view of protection against technical penetration, arrangements at the White House present certain advantages. The greatest advantage is the relative geographic isolation of the White House from other buildings, particularly non-Government controlled buildings. This spatial separation presents practical problems to potential penetrators (a) in transmitting intercepted information out of the White House, and (b) in locating and manning a listening post. Also, the present protection program of the Secret Service and the White House Police, oriented largely to protection of the person of the President, provides almost as a side effect a measure of protection against technical penetrations.

On the other hand, there are a number of conditions which make the White House a difficult facility to defend against technical penetrations. First, even sensitive areas of the White House are relatively open to people with varying degrees of clearance and control. White House Police statistics show the following numbers of people moving through the White House in FY 1964:

- 5,000 Tradesmen, vendors, construction and repair personnel,
TV and radio technicians, etc., service the White
House in a year, many returning a number of times
(25,000 separate entries)
- 49,000 Official visitors, U. S. and foreign

~~SECRET~~

~~SECRET~~

9

- 2,000 Military support personnel, including communications personnel, mess stewards, chauffeurs, and bands
- 1,700 Members of the press, TV, and radio, including those from Communist and other foreign countries, with press passes.

These are in addition to about 1,000 other people having White House passes (professional and administrative staff, domestics, char forces, gardeners, agency officials, etc.), 51,000 guests at social functions, and 1,800,000 public visitors and tourists, some of which are given private tours through sensitive spaces by personnel assigned to the White House.

In terms of the study, the large number of construction and repair workmen, particularly telephone maintenance men, electricians, and TV technicians are of particular interest. On a recent week-end, there were seven different contractors and ninety workmen in the West Wing and the Mansion, and this is considered a typical level of activity. The fast pace of such activity often complicates technical surveillance. For example, a quick decision to have TV coverage of an event can result in 40 - 50 technicians setting up lights and cameras and running cable in the President's office and adjacent areas for a period of several hours. TV coverage is liable to be followed almost immediately by a high-level meeting in the President's office with no time in between to conduct a countermeasures search.

~~SECRET~~

Lastly, the White House is an old facility. Its space has been altered and re-altered on a piecemeal basis many times. Also, space is overcrowded and allocated without much consideration to security - e.g., recording room under the President's lounge-office; press share an adjoining wall with Mr. Moyers; messengers and duplicating facilities adjoin the Situation Room. Telephone, electrical and other wiring, and piping systems have been added over the years without any systematic effort to remove the old. "As-built" engineering drawings which are essential in identifying deviations are often not available.

why not then?

General assessment of present protection

In marked contrast to the need for good technical security, there is actually no coherent security program at the White House, and little indication that one is being developed. Basic problems are:

- Responsibilities for security are diffused.
- There is no one in charge.
- There are gaps in coverage.
- The efforts to provide technical security countermeasures suffer from lack of authority, technical competence, and manpower.

~~SECRET~~

~~SECRET~~

11

- The telephone companies and the White House Communications Agencies are efficient providers of communications, but, left to their own devices, they have given little consideration to sound security. At present, they lack understanding of the problem.
- The combination of measures to clear and control movements of people is not adequately related to the needs to protect against technical penetrations.

Major specific findings

The survey found a number of potentially dangerous conditions which illustrate a lack of attention to technical security problems and which should be remedied as soon as possible:

1. Special problem reported in the Director's Memorandum to Mr. Bundy, dated April 21, 1965.

2. In checking the private line extensions off the White House switchboards to the residences of the 12 key advisors to the President, the following conditions were found:

a. Secretary McNamara's private line was found to run along the back wall of the Finnish Embassy. An employee of the Embassy indicated he knew of this condition and stated casually, "We listen to him ^(Secretary McNamara) all the time." The dangers to this service, since rerouted, were (1) "cross-talk" from Secretary's line to the line to the Embassy which ran in the same cable (this can be ^{probably} picked up by proper amplification on the regular Embassy telephones), or (2) an inductive tap (see ^{Chapter II} ~~Appendix~~ page ____).

I think I would have said. People who want to know.

Is it?

~~SECRET~~

b. Secretary Rusk's two private White House lines "appear" eight times. These appearances are accessible, and a potential operation would be masked by the wooded area through which the service passes. One of the line appearances was on the property of a registered agent of the Dominican Republic (see Chapter II, page ____).

fixed?

2. Long distance telephone service to the LBJ ranch is highly vulnerable to intercept in the open wire carrier and microwave links between Austin, Texas, and Johnson City.

has this been fixed?

3. Clear text of classified messages was recovered by reading emanations from secure teletype equipment at the LBJ ranch on the open wire power lines from the ranch house for a distance of 3/4 mile. We know it went much further. Recovery of the same information was made from the telephone lines and microwave system going from the ranch to Austin. These conditions have since been corrected.

4. The secure teletypewriter equipments in the White House communications center and the International Situation Room also were found to be high-level "radiators," which, in conjunction with improper intermixture of secure and non-secure telephone lines, provided potential paths for transmission of clear text information of encrypted messages out of the White House. Both of these facilities as surveyed do not conform to Government-wide security standards.

fixed?

5. The counter audio survey has found numerous places where there is acoustical leakage from sensitive offices. Conversations in Mr. Moyers' office could be heard through the wall into a press area and through an old sink pipe down into the dispensary below; similarly, an unused pipe conveys intelligible sound from the Cabinet Room to a Secret Service squad room below.

fixed?

6. Presidential and other West Wing telephone service runs through terminal rooms which also serve press, TV, radio, Muzak, and other services going directly out of the White House (not through the manual switchboards). Wiring conditions in these rooms were such that it would be extremely difficult to identify an improper cross-connection or tap.

7. There are direct, live audio lines from the Cabinet Room to television and radio networks. Such lines also appear in the hall outside the President's office. The potential of a quick connection of a microphone to one of these lines constitutes a hazard.

8. Telephone maintenance men and GSA electricians permanently assigned who have the greatest access to vital telephone and electrical systems do not receive the FBI full field investigations given to regular White House employees, including cooks and gardeners. Technicians (telephone, electrical, and TV-radio people) not permanently assigned are not given adequate escort to protect against penetration.

~~Numerous other conditions which require attention are described in the appendices.~~

9. In the survey, an open safe containing Top Secret material was observed, left open over night; more significant, perhaps, the safe which had been in use for _____ still had the basic factory combination (50-25-50).

Assessment of risks and vulnerabilities

Based upon discussions with appropriate officials involved in various aspects of White House security, there has been no concrete evidence of hostile audio surveillance activities directed against the Presidency in this country. None has been uncovered in the comprehensive counter audio survey to date. However, even after the completion of the comprehensive survey, there cannot be 100 percent assurance that the White House is free of audio surveillance devices.

On several occasions, questions have been raised as to the relationship between audible clicks on telephone lines and possible tapping. Based upon a study by the Chesapeake and Potomac Telephone Company, the greatest source of clicks is the operator checking the line to see if calls are completed. Clicks also result from maintenance people checking lines and very infrequently from natural phenomena. A telephone tap generally cannot be detected audibly.

can operator hear?

However, given the problem areas, the state of the protection program, the threat of technical penetration appears to be as follows (generally ranked from most to least vulnerable):

1. Most vulnerable are mobile radio telephones in cars, helicopters, and aircraft. It must be assumed that the Soviets monitor all radio telephones in the Washington area from their Embassy. The Presidential aircraft would also be a prime monitoring target, and the Steering Group has seen transcripts of classified conversations from the aircraft to the

White House recorded by an Air Force contractor, Radio Liberty, in Iowa. The LBJ network in Texas can be monitored by anyone with simple radio equipment with a 35-mile radius.

2. Normal (in the clear) telephone conversations on the open wire ^{and} carrier and microwave links between the LBJ ranch to Austin can be tapped or monitored with comparative ease and little chance of detection.

3. Private line telephone service to residences and offices can be monitored in the normal course of business by operators at the White House switchboards and by maintenance men and operators at the telephone exchanges (usually two or three exchanges) where the lines are tagged for special service. The lines to residences are vulnerable to tapping in the last leg near the residences where they become easily identified (they usually follow the same routing as normal telephone service). The lines also frequently appear in questionable places as noted for Secretaries McNamara and Rusk.

4. Telephone service for the Executive Office Building (EOB) is more vulnerable to intercept than that in the White House. First, it is served from a terminal room in the basement where wiring conditions, and hence the ability to spot cross-connections, are exceptionally poor. Second, the building was completely open to the public during office hours up to about three years ago, and it is still more open to entrance and movement within it than the White House. Third, the service can be monitored by operators in the Lafayette exchange. It should be noted that the White House lines to the offices of Secretaries Rusk, McNamara, Fowler, and Udall pass through the basement terminal room and that most of the NSC staff

supporting Mr. Bundy (all when the study began) are served through this room and the Lafayette exchange.

5. Given the number of people moving in and out of sensitive spaces, and the general situation at the White House, the introduction of a small, self-powered radio transmitter which can be quickly concealed by people having limited access (workmen, TV technicians, char forces) presents a possible form of technical penetration. Likely listening posts would be TV or other trucks parked in West Executive Avenue, little-used spaces in the attic of the EOB, or buildings along 17th Street or "H" Street N.W. The miniature recorder (cigarette package size) which could be easily concealed, ^{also} presents a threat.

6. Presidential telephones could be cross-connected or tapped in two terminal points in the White House where his service is intermixed with other telephone service not going through the switchboard, ^{where there are} and ^{the} numerous spare pairs in the outgoing cables ~~are a problem~~. In addition, all Presidential calls through the White House switchboard are accessible ^{in the EOB} at the switch room and the switchboard, ~~in the EOB~~. Access to these points would be required.

7. Use of wired microphones, carrier transmitters, or compromised "hot" telephones present substantial problems of transmission in and out of the White House, but should not be ruled out given present ^{wiring} conditions. Extensive access to telephone and electrical systems would be required.

8. Sophisticated penetration techniques such as infra-red windowpane pickoff, laser beams, lip reading by telescope, directional parabolic microphones, etc., appear to be limited by physical conditions at the

White House and the state of the art. However, advanced developments in some of these areas must be carefully watched and considered in developing future protection programs.

9. The three underground "feeder" telephone cables from the White House to the downtown and mid-town exchanges and more particularly the 100 pair cable to the mid-town exchange offer relatively attractive possibilities for tapping which are made easier by tagging all White House lines in the exchanges to ensure good service. The cables themselves could be tapped in a little used manhole or by means of a tunnel into the cable vault. The latter would be quite difficult and costly for a tapper, but the yield could be high, and detection might be difficult.

IV. MAJOR CONCLUSIONS AND RECOMMENDATIONS WITH RESPECT
TO GENERAL SECURITY AND AUDIO SURVEILLANCE COUNTERMEASURES

Overall security responsibility

Fundamental to the conditions found by the survey is the fact that there is no central authority to direct and integrate the fragmented security functions. Security files for White House personnel are reviewed by Mr. Watson; Mr. Moyers has responsibilities for approving White House pass issuance and for communications; Mr. Bundy controls the handling of most classified documents; Secret Service with the White House Police provides certain physical security; Secret Service exercises responsibility for audio countermeasures for most of the White House and security pertaining to administrative (non-military) communications; the White House Communications Agency (WHCA) provides security for its communications; and the FBI performs full field investigations and specific counter audio and communications investigations on call.

This diffusion of responsibility has resulted in gaps in the overall effectiveness of the White House security program. It certainly is not conducive to developing a program to meet the increasing technical threat.

It is recommended that:

1. Responsibility for physical security, telephone security, audio countermeasures, and personnel clearances should be clearly assigned to a single Presidential assistant. With proper staff support as recommended, the security assignment would take only a small portion of the assistant's time, but his responsibilities should be clear.

2. Staff support for the designated Presidential assistant should be provided by a professional, high-grade security officer reporting directly to such assistant and responsible for ensuring that a comprehensive security program is established, appropriately coordinated, and effectively maintained. The security officer should have broad experience in the several areas of security and should have a small staff of two people to assist him.

Audio countermeasures program

The Secret Service program to protect the President from technical eavesdropping began in the early phases of World War II. Protection of Presidential privacy was assumed to be a logical extension of the statutory responsibility "to protect the person of the President" and his immediate family. Yet, as late as 1962, there were only two people concerned with audio countermeasures. In the last year, the number has been increased to six, although only about 50 percent of the time of these men is spent on audio countermeasures per se.

However, to this day, there is no statutory authority or written directive assigning Secret Service any responsibility for audio countermeasures.

Also, there has been no guidance or direction from outside the Secret Service (either the White House or the Treasury) indicating the degree of emphasis to be given to this function or checking to see what was being done. It is not surprising that the Secret Service management, oriented largely to protective and investigative functions, has not allocated enough of its scarce budgetary and manpower resources to the countermeasures effort. The program has tended to drift along with the following results:

~~SECRET~~

20

- Inspections from President's office on down have been cursory and too infrequent.
- There are important gaps in coverage; e.g., the offices of the NSC staff and the residences of the Vice President and key White House aides.
- Personnel, often shifted from investigative functions, have inadequate technical training.
- There is no base of technical information concerning the White House facilities.

Chapter I contains a detailed review of the program and 16 specific recommendations for improvement.

There are good reasons for having the Secret Service provide "in-house" audio surveillance countermeasures capability as many of these functions can be fitted in most easily with other activities related to protection of the President and the White House. However, the basic unknown is whether a "police" agency like Secret Service can give proper support and direction to technical activities and whether it can attract, retain, and direct the technical competence required for the handling of the more sophisticated audio threat anticipated in the next few years. It is especially important that the director of the technical security program be highly qualified in engineering or the physical sciences.

We conclude that the Secret Service can and should develop an effective countermeasures program, if the recommendations herein for strengthening its capabilities in this field are implemented. The alternatives --

~~SECRET~~

~~SECRET~~

assigning responsibility for this function (a) to WHCA, (b) to a new civil service unit attached to the White House or some office in the Executive Office of the President, or (c) to an operating agency like State, Defense, or CIA -- were considered and rejected as less desirable. If it appears, however, that after a year the Secret Service program has not developed the technical leadership and competence required, alternative arrangements should be reconsidered.

It is recommended that:

3. Responsibility for the audio countermeasures program in the White House (including ^{the East Wing Shelter} ~~all regular telephone facilities provided by WHCA~~) and at residences of the Vice-President and key Presidential staff should be clearly assigned by Presidential memorandum to the Secret Service, and execution should be under the direction and guidance of the proposed White House Security Officer. The intelligence community should provide staff and equipment to supplement that of the Secret Service on request.

4. Within Secret Service, the technical security function should be separated from the Protective Research Section and given greater organizational emphasis.

5. Efforts should be made to obtain a highly qualified technical director for the program. If Secret Service is not able to hire such a person, he should be detailed for periods of two - three years from an agency in the intelligence community having substantial technical programs.

~~SECRET~~

~~SECRET~~

6. The White House Security Officer should be a permanent member of the Technical Surveillance Countermeasures Committee of the U. S. Intelligence Board in order to keep abreast of developments and to obtain advice and assistance from the Committee as needed. Similarly, the technical director of the Secret Service countermeasures program should attend meetings of the Research and Development and Audio Countermeasures Sub-Committee.

never get them

7. Staff of the Secret Service performing the technical security function should be increased by at least five people, over and above the present complement of six. All staff should be technically trained, and at least half of them should be graduate engineers.

8. The frequency and coverage of the audio countermeasures program should be extended and intensified as recommended in Chapter I. The Secret Service should also be responsible for surveillance of buildings around the White House which might be used as possible listening posts.

9. Assistance in meeting any unique research and development requirements for countermeasures at the White House should be sought from appropriate agencies, particularly the Advanced Research Projects Agency in Defense.

10. The Secret Service countermeasures program should be reviewed in a year by a committee chaired by the Director, Office of Science and Technology, to ensure that progress is being made toward developing an effective program in terms of the threat. The Director should make recommendations to the President through the designated Presidential assistant for security.

~~SECRET~~

Security aspects of construction and repair activities

Many people in the White House initiate changes in telephones and physical arrangements on a rush basis with little consideration given to security effects of the action. These changes may be implemented by the White House Communications Agency (WHCA), the telephone company, GSA, the National Park Service, the Navy, or some other agency. It is not an infrequent occurrence that the first Secret Service hears of a project is the daily notice that contractor employees will arrive on the job. Once features are installed, it is more costly to make changes which might be required for security reasons.

It is recommended that:

11. Regular procedures be established for coordinating physical changes in advance with the proposed Security Officer, especially all changes in telephones and electrical systems.

Personnel clearances and control of people

In the last few months, clearer and more effective procedures for reviewing FBI investigations and approving assignments to the White House staff and military personnel have been established. However, there are still somewhat diffuse authorities for conducting investigations, reviewing reports, and issuing passes, ~~especially~~ for maintenance people, vendors, and tradesmen.

~~The Steering Group has been particularly concerned about the system of clearing and granting access to technicians, particularly those who have extensive access to telephone and electrical systems.~~ *(See Chapter I)* ~~About 60 telephone~~

~~SECRET~~

~~maintenance employees having permanent White House passes are not given full field FBI investigations, but are investigated by the Military District of Washington, U. S. Army, at the request of the telephone company. Secret Service issues a pass on the basis of certification of clearance by the company with no further review of the files. Secret Service also grants passes to maintenance employees of GSA and the National Park Service on the basis of review of files furnished by those agencies. Contractor personnel, including electricians, are given limited checks by Secret Service (checks of FBI and local police criminal files) often after the man is already at work. TV and radio technicians are given permanent press passes after checks of FBI and police criminal records and, if the person has foreign connections, CIA files are checked.~~

Control of such people within the White House from the viewpoint of preventing technical penetrations is somewhat haphazard. Permanently assigned telephone people having White House passes have free run of the facility without inspection, except for the President's office. When, for particular rush jobs, additional telephone people are brought in they are placed under the supervision of the pass holders for most areas. GSA maintenance people with passes are treated similarly. Other workmen with visitor badges are escorted, often rather loosely, by a White House Policeman who has not been trained in identifying technical penetrations, and whose main objective is to see that the men do not wander off toward the President. The Steering Group has observed cases where the escorting officer sat in the hall watching a door from the outside while workmen operated freely and unobserved in sensitive spaces.

It is recommended that:

12. The proposed Security Officer be given authority to establish and maintain appropriate and consistent security standards for investigation and review of all persons having duties in the White House or access to it.

13. Authority for granting clearances and issuance of White House passes should rest with the proposed Security Officer under the supervision of the designated Presidential special assistant for security.

14. All people permanently assigned to the White House, including telephone company and GSA maintenance personnel, should be given full field FBI investigations (except Secret Service, White House Police, and military personnel who are investigated otherwise).

15. All workmen who have prolonged access to the electrical or telephone systems serving sensitive areas, who have not been given full FBI investigation, should be escorted by technically trained members of the Secret Service countermeasures unit.

Other technical and physical security measures

A considerable number of technical and physical security studies, which are outside the scope of this survey, need to be made. The proposed Security Officer should be responsible for initiating:

- A comprehensive program to map sensitive spaces of the White House acoustically and electrically.

- A systematic program to identify and remove if not in use all telephone, electrical, and other wire in the White House. Consideration should be given to use of noise generators on wires which are considered potentially dangerous but which cannot be removed.
- Tests to determine the feasibility of background masking "noise" which might render technical surveillance more difficult.
- A comprehensive "base" physical security survey of the White House (this is being done in part in this survey).

~~SECRET~~

Classified document handling

The survey was concerned with the adequacy of security of procedures for handling classified material in the White House and the LBJ ranch. The survey did not deal with the efficiency of this process or with the handling of unclassified documents.

By far, the larger percentage of total volume of written material received and handled within the White House is unclassified, although much of it is sensitive. As a general rule, White House personnel appear to operate on the premise that all papers addressed to the President are automatically "Confidential" and "Personal" in nature, and this general approach undergirds the system for handling formally classified documents.

The survey revealed that there are no written procedures now in effect for handling classified documents in the White House. However, a less formal system ^{for control and improvement of such documents} has evolved, centered primarily on Mr. Bundy's operation, which appears ~~very~~ effective considering the unique situation of the White House, the pace at which papers are handled, and the lack of any overall security authority noted above. Although the committee was informed of lapses ^{in this process} which have occurred in the past, the people with whom the problem was discussed exhibited a reasonable and consistent understanding of the present system and an excellent awareness of the need to protect documents.

~~SECRET~~

~~SECRET~~

28

We have examined the applicability of certain recognized techniques of securing classified documents - e.g., central control and registry system, multiple receipts, follow-up tickler arrangements, complete in-house facilities for handling and storage. These do not appear realistic or advisable for the White House in view of the volume of paper moving through the White House, the rapid demand for information, the late hours worked, and the shortage of space. In particular, the incremental security from an attempt to pass all classified documents through one central point in the White House does not appear to outweigh the additional restrictions in the speed of handling the documents. This assumes, however, an operable and consistent decentralized system.

With respect to organizational responsibilities, it is clear that the President's Assistant for National Security Affairs will, by the very nature of his task, have to handle the vast majority of classified documents, especially those involving special categories of clearances. It was indicated that about 95 percent of classified documents flow ~~into or~~ through the Bundy complex. It, thus, makes sense to concentrate the handling of such paper in his office, backed by the NSC staff, as is now the case. However, overall responsibility for ensuring that there is a

~~SECRET~~

~~SECRET~~
~~SECRET~~

29

system, that it fits adequately with the rest of the physical security program, and that it is adequately understood, especially by secretaries and administrative assistants in all offices, should be exercised by the proposed White House Security Officer.

An example of the type of problem requiring attention of the Security Officer is that of securing classified documents after hours. The committee was advised that responsibility for securing classified documents at the close of the day resides in each office and that each office organizes its own checks on performance. However, the Steering Group has observed enough instances of Top Secret materials being left on desks at night to conclude that this is a common occurrence, ~~with some~~ ~~Secret materials~~. The physical protection program provided by the White House Police does not appear to warrant this confidence, especially given the number of loosely escorted workmen and char force personnel wandering around the White House on a given evening.

We have reviewed with special care the handling of the highly classified material which becomes a part of the President's "night reading" file, particularly the State Department's "Evening Reading" and CIA's "President's Daily Brief," the latter containing COMINT and other highly sensitive material. It is concluded that, although these materials appear to be handled with awareness by all concerned, the security of the process would be improved by reducing the number of people who handle or have access to these materials on the way to the President. For

~~SECRET~~
~~SECRET~~

~~SECRET~~

example, these materials, generally received in Mr. Bundy's office between 6:30 and 7:00 P.M. each evening, are forwarded to the President's secretary for inclusion in the night reading file, delivered by a White House messenger to the Head Usher, handed to the Doorman, who either gives them to the Sergeant valets on duty or takes them directly to the President's private quarters. If the President is out for the evening, the documents remain untended on his bed until his return to the White House.

It is recommended that:

16. The proposed Security Officer should establish policies and procedures for the handling and storage of classified material in the White House and that staff, particularly administrative staff, are familiar with these.

17. Highly classified documents for the President's night reading should be held in the Situation Room when the President is out for the evening and should be delivered to the President's quarters by the Watch Officer when notified of the President's return.

18. The procedures for checking and locking up classified documents at night should be ~~reviewed by the Security Officer~~ strengthened. The role of Secret Service in this process should be clarified.

~~SECRET~~
SECRET

~~SECRET~~

V. MAJOR CONCLUSIONS AND RECOMMENDATIONS
WITH RESPECT TO TELEPHONES AND COMMUNICATIONS

Basic findings

Communications are a vital instrument of Presidential command, and effective communicatings, starting with the systems closest to the President, deserve high national priority. Important attributes of an effective system are privacy and security. All men deserve privacy in communications, but the President of the United States requires the best protection possible.

The telephone security problem at the White House is inherent in the system. The present telephone system at the White House grew like Topsy and certainly was not designed with security in mind. There are (a) too many switchboards with too many operators who can overhear conversations, (b) too many terminal boards where cables from sensitive telephones intermix with service going directly out of the building, and (c) too much excess wiring and equipment lying available. Records are inadequate, and no one knows the whole system.

~~SECRET~~

~~SECRET~~

32

WHCA's "Signal" switchboard has already reached its capacity, and the White House switchboard at the present rate of growth in service is expected to reach saturation next year. Ever since the White House board was moved to the EOB in 1962, the system has been considered "interim" by the Chesapeake and Potomac Telephone Company. ~~The Company has been awaiting a decision from the White House to develop an improved system.~~

why wait?
it's given?

Need for overall responsibility

As in the general security area, there is no clear responsibility for planning communications in the White House, particularly technical planning.

No single person is responsible for integrating Presidential and White House staff needs in day-to-day and emergency situations and seeing that appropriate plans are developed to meet them. It is believed that communications are so important to the President that general responsibility should be placed in one Presidential assistant. This assistant, however, must be given strong technical support.

provide

to the Presidential Assistant

The most logical official to ~~the~~ provide technical support is the Director of Telecommunications Management (DTM), who already performs a number of communications functions for the President, including the development of Presidential requirements for inclusion in technical planning for the National Communications System (NCS). With a small staff of competent engineers, the DTM could work with the telephone companies, WHCA, the Defense Communications Agency, and others to see that longer term system capabilities provided the President are modern, secure, and adequate to his informational and command needs. In planning the security features, the DTM should work with the proposed Security Officer and technical director of the countermeasures program.

~~SECRET~~

It is recommended that:

1. Responsibility for Presidential communications should be placed clearly on a single Presidential assistant, preferably the same person having general security responsibility.
2. On technical matters, such as the planning for facilities and capabilities, and security, the designated special assistant should look to the DTM for support. The DTM should acquire the necessary technical competence to perform this task.

Planning for a new, more secure system

It is strongly in the nation's interest to see that the President has an effectively planned communications system with the best features of privacy and security built into it from the beginning. Basic questions with respect to a new system are (a) whether it should be self-contained (electronically segregated and physically secured), and (b) how much of the Executive Office of the President it should embrace. The long-run trend will be to move more activities directly supporting the White House into the EOB and Federal Office Building (FOB) No. 7. It would appear prudent in telephone planning at this time to consider the White House - EOB - FOB No. 7 as a single complex served from a central switchboard in the EOB. This switchboard could have dual capabilities --

~~SECRET~~

(a) manual capability serving the President and top staff as determined by later studies, and (b) a flexible, rapid dial system which could ring anyone in the complex by dialing only two or three digits.

This single system should largely replace the three switchboards now in use with considerable savings in the number of operators, trunking, and line costs. In fact, the C&P Telephone Company has estimated that such new service could be rendered for approximately the same annual recurring cost as that for the present system. In the system studies which are required, these cost factors should be carefully weighed.

It is recommended that:

3. The designated Presidential assistant for communications should request the DTM to work with the telephone company, WHCA, Defense, GSA, and the White House Chief Clerk to develop and recommend a rational telephone system for the White House - EOB complex, *Consideration of* with the following security features:

- a. A self-contained system serving the whole White House - EOB complex and physically secured;
- b. A combination of manual operation and a flexible dial system so that calls can be made without going through the operator.
- c. An automatic disconnect capability, even for the dial portion, so that when the inside telephone is hung up, the line into the White House does not remain open to outsiders.
- d. Some form of operator disconnect on calls that have been established so that the operator cannot re-enter the circuit except on recall by the parties.
- e. Maximum cryptographic security for links outside the complex.

~~SECRET~~

~~SECRET~~

Crypto-Secure Telephones

The only way that telephone calls outside the White House compound can be completely protected is through use of crypto-secure voice systems. Marked improvements in quality are being made, and the new KY-3 telephone is equal in quality to that of regular telephones. These should be installed at vital White House links as soon as feasible (KY-3 facilities now exist from Mr. Bundy's office to the Secretary of State and to the ranch).

However, the new secure voice service should not be made available to the President until it has been proven elsewhere and will clearly meet his needs. There has been a tendency in the past to use the White House as a proving ground for completely new ~~pieces of~~ communication equipment, before the function and security of the equipment has been established.

The present proposal to install a secure facsimile capability between the Pentagon and the Situation Room appears to be an example. The security characteristics of this equipment should be thoroughly demonstrated before installation.

It is recommended that:

9. KY-3, high-quality, secure telephones be installed, as soon as feasible in circuits between the President and offices and residences of key national security advisers. Secure voice capabilities for Presidential aircraft, helicopters, and cars should be developed and installed when ready. The critical point is the acceptance and use of these telephones once installed.

Is this about
J.P.?

Responsibility for telephone security at the White House

For historical and practical reasons, there is a split responsibility for providing regular, non-secure telephone service at the White House, and this split complicates the fixing of responsibility for telephone security. The White House board, manned by civilian operators under the direction of the White House clerk handles the majority of incoming and outgoing traffic (reportedly 90 percent). WHCA handles the balance through the Signal Board. WHCA also has operational responsibilities for crypto-secure communications at the White House and for all communications at the LBJ ranch and while the President is travelling. The local telephone company installs and maintains most of the equipment used by both services.

The present diversity of facilities and responsibilities does not appear to represent the most rational pattern. Before new systems are planned and implemented, there is a great need to determine a more optimum balance, especially as more crypto-secure communications are introduced.

WHCA is a very effective communications agency providing a vital element of Presidential support. However, its effectiveness is weakened by the lack of policy guidance from the White House; what guidance there is comes from a wide number of sources.

It is recommended that:

3. The designated special assistant for communications be the focal point for guidance to WHCA. With technical support from the DTM, he should initiate ^a ~~and~~/review of the relationship between WHCA and other elements providing regular telephone service at the White House.
-

Secret Service has exercised some responsibility for the security of telephone service running through the White House board as a part of its audio countermeasures activity. However, until 1959, the Steering Group was told that the telephone company kept terminal rooms in the White House locked and did not allow Secret Service inspection. Since that time, the company has made more information concerning the system available to the Secret Service, but not enough to permit a thorough assessment of security.

The intermixture of telephone service makes the drawing of lines of responsibility for telephone security between the Secret Service and WHCA a difficult matter, especially if there is a move to a combined switchboard in the EOB. Since a major portion of the telephone security is encompassed in a strong audio countermeasures program, we believe that the Secret Service should assume responsibility for security of all non-crypto-secure telephones. WHCA should continue its responsibilities in the area of crypto-secure telephones. ~~WHCA should continue its responsibilities in the area of crypto-secure systems.~~ However, even this ^{division} ~~line~~ will tend to blur in the future as more crypto-secure voice service is introduced into White House offices, especially if secure and non-secure service is eventually provided in the same "call director."

As indicated earlier, we recognize the problems for Secret Service management posed by the addition of these and other technical responsibilities. In the communications area, it would be expected that the Secret Service would obtain highly qualified technical leadership and would call on staff of the DTM, WHCA, and others as needed.

It is recommended that:

4. Under the guidance and supervision of the proposed White House Security Officer, the Secret Service should, as a part of its audio countermeasures activities, be responsible for protection of all White House telephones (including those operated by WHCA) which are not cryptographically secure.

Other communications recommendations

5. Until secure phones are available, the Secret Service should check the private line service to key residences of White House officials through the exchanges and from the last exchange to the residence in order to identify and to have corrected obviously insecure conditions.

6. In any case, key staff of NSC supporting Mr. Bundy should be served by the White House board, rather than through existing EOB terminals and the downtown exchange.

7. The WHCA recording studio should be moved away from the President's office.

8. The speaker phones being used by the President and his immediate staff should be tested by NSA to be sure they are not radiating information out of the White House. (NSA has initiated such tests.) Steps should be taken to see that the "live" audio from these speaker phones ^{does} not get beyond the Presidential telephone frame room, *as is now the case.*

Communications from the LBJ Ranch to Austin

The Steering Group has explored with telephone company staff the possibility of installing a combination of (1) a digital carrier system (such as the T1 carrier currently in use in the Bell system), and (2) crypto-secure facilities to protect the LBJ ranch - Austin microwave link. These specially protected circuits could be used for particularly sensitive conversations, although the long-distance private line circuits from Austin to Washington will remain as vulnerable in the exchanges as they are today.

It is recommended that:

6. NSA with the assistance of the Bell System explore the feasibility and cost of providing an appropriate number of secured circuits for ^{the vulnerable LBJ} ranch - Austin link and to make recommendations to the designated special assistant for communications.

Compromising radiations (TEMPEST)

The encrypted communications at the White House Communications Center in the East Wing, as found by the survey, had been installed by WHCA with little attention to the problem of compromising radiations. What is more, WHCA had not requested a TEMPEST check at the White House since 1962, although standing procedures called for inspections at least every year. The preliminary inspection of the WHCA communications area in the East Wing Shelter, initiated as a part of this survey, showed a number of unacceptable practices, including the use of a high-level teletypewriter cryptographic equipments which under previous tests have been proved to produce compromising emanations. Corrections have since been made, and a TEMPEST check has been completed.

Similar conditions were found in the International Situation Room. However, the scope (and potential pick-up) of these radiations is considered potentially more dangerous, because the Situation Room is at ground level on West Executive Avenue. TV trucks and other vehicles parked in the area pose a potential threat. These problems still await correction, after which a TEMPEST check should be made.

The situation in the WHCA communications trailer at the IBJ ranch was basically the same as that at the White House - i.e., the cryptographic equipment was programmed for high-level signal operation. Readable signals were obtained by Army technicians near the overhead, open wire carrier three quarters of a mile from the ranch. It is apparent that from this that the "clear text" radiations were getting into both the open wire carrier and microwave system to Austin. These conditions have been corrected.

It is recommended that:

16. The WHCA facilities be regularly inspected to insure continued compliance with TEMPEST standards and to keep abreast of state-of-the-art advances, ^{and these} ~~TEMPEST tests at the White House~~ should be supported by NSA.

17. WHCA personnel should receive continuing technical guidance from Army Security Agency, NSA, and others to keep abreast of advances in the TEMPEST and communications security field. ~~Prior to operational usage of the secure television or facsimile system, it should be TEMPEST tested.~~

41

~~SECRET~~

13. Prior to any additional secure communications systems or equipment being installed, including the proposed secure television and facsimile systems, detailed plans should be prepared and concurred in by the proper TEMPEST-trained command.

White House office machines

The survey group attempted to identify automatic office equipment which might radiate recoverable intelligence. On inspection, it was determined that the Xerox machines used for classified information in the White House and the EOB constitute no risk. However, the two Flexowriters, two Royaltypers and four Robotypers used in room 59 of the EOB under the administrative control of the White House do represent a potential hazard.

It is recommended that:

13. Controls should be placed on the above-mentioned machines in room 59 to insure they are used only for unclassified or, at most, confidential information.

14. If, in the future, any office machines are installed, particularly if this is electronic data processing equipment, consideration should be given to the resulting possibility of compromising radiations.

~~SECRET~~

4

THE WHITE HOUSE
WASHINGTON

~~SECRET~~

May 6, 1965

MEMORANDUM FOR MR. BUNDY

SUBJECT: Communications Security Study

1. Jim Clark has delivered the President's copy of the Communications Security Report to me. As you might suspect, it is a hefty document.

2. My own inclination is to hold off on sending it to the President for a few days. First, the Report has been many months in the making and a few more days won't matter. Second, it should probably get careful, cool, close study and I suspect that neither the President, you, nor I is going to be able to do this until the Dominican situation quietens a bit.

OK / 3. Therefore, if it is O.K. with you, I will (a) hold the Report for now, (b) do some study and staffing on it over the weekend, and (c) pass it to you the first of next week along with a recommendation as to the next step we ought to take.

GC
Gordon Chase

DECLASSIFIED
E.O. 13292, Sec. 3.4
NSC Memo, 1/30/95, State Guidelines
By jc, NARA, Date 3-18-05

~~SECRET~~

5

May 3, 1965

STATUS OF NSAM 315 SURVEY

	<u>Director's Memorandum</u>	<u>Summary Report</u>	<u>Complete set including chapters</u>
Original	President		
Courtesy (Copy 1)	President	President	
Copy 2	Director	Director	
Copy 3	Mr. Bundy		Mr. Bundy
Copy 4	Mr. Chase		Mr. Chase
Copy 5	Mr. Chase	Mr. Chase	
Copy 6	Mr. Chase	Mr. Chase	
Copy 7	Mr. Chase	Mr. Chase	
Copy 8	Dr. Hornig		Dr. Hornig
Copy 9	Mr. Carey/ Director		Mr. Carey/ Director
Copy 10	J. W. Clark		J. W. Clark
Copy 11	J. W. Clark	Mr. Chase	
Copy 12		Mr. Chase	
Copy 13		Mr. Chase	
Copy 14		Mr. Chase	
Copy 15		Mr. Chase	

Determined to be an
administrative marking
By jc On 3-18-05

CONFIDENTIAL

April 30, 1965

MEMORANDUM FOR MR. VALENTI

SUBJECT: New Telephone System for the White House

1. From all I have heard about the matter, there is, in fact, a genuine need for a new White House Board, and I am in favor of giving the Telephone Company a go-ahead on initiating design studies.
2. As for the BOB Study Group (Jim Clark's group), an informal check indicates that the Group believes that the development of a new telephone system in the White House (including a new Board) would be highly desirable. As a matter of fact, in its report, which is due to be submitted in the near future, the BOB Group will recommend that design studies be initiated on a new system.
3. One important point to be made is that someone from the Government should be designated to stay in close touch with the Telephone Company as it proceeds with its work. In this regard, the BOB Group will be recommending that the Director of Telecommunications Management (General O'Connell), under the direction of a Special Assistant to the President, be designated for this job; the General would also tie in closely with security types, Bill Hopkins, WHACA, and other appropriate people.

McG. B.

CONFIDENTIAL

DECLASSIFIED
E.O. 13292, Sec. 3.4
NSC Memo, 1/30/95, State Guidelines
By je, NARA, Date 3-21-05

~~TOP SECRET~~
EXECUTIVE OFFICE OF THE PRESIDENT
BUREAU OF THE BUDGET
WASHINGTON 25, D.C.

M-50/65-TS/6⁸³¹
C.5
8

APR 30 1965

MEMORANDUM FOR THE PRESIDENT

Subject: White House Security Survey

We have completed the survey of technical and physical security protection for the Presidency in accordance with NSAM 315. The survey covers arrangements for protecting the White House and, to a lesser extent, the ranch and the Executive Office Building, against possible technical penetrations, i.e., invasions of privacy and security through clandestine eavesdropping devices and telephone taps.

I have been quite disturbed to discover the existence of so many weaknesses in present security arrangements at the White House and the consequent exposure of your security and communications to technical penetration. Fundamental to this condition is the lack of clear responsibility or decision points for these matters.

The report identifies measures which should be taken, now and over a longer period, to tighten up and improve the security of the White House. I strongly recommend that you personally read the summary report.

In the survey, we have given careful attention to costs as well as benefits of the proposed improvements. I am satisfied that costs of actions growing out of the survey can be covered by appropriations available to appropriate agencies (primarily Defense and Treasury) in FY 1966.

Our general ground rules were to effect security improvements as the survey progressed, and examples of such improvements are noted in the attachment. However, fundamental improvements must await White House decision.

Mr. Bundy and I are ready at any time to discuss these matters and appropriate steps to carry out your decisions.

(signed) Kermit Gordon
KERMIT GORDON
Director

Attachment

DECLASSIFIED
E.O. 13292, Sec. 3.5
NLJ/RAC 05-48
By isl, NARA, Date 3-4-08

~~TOP SECRET~~

EXCISE	GROUP
1	1
DELETED	1

~~TOP SECRET~~

M-58/65-TS/6A
C.5

Attachment

EXAMPLES OF SECURITY IMPROVEMENTS
MADE IN THE COURSE OF THE NSAM 315 SURVEY

1. Fundamental reductions have been made in possible compromising radiations from communications equipment handling classified material at the White House and the LBJ ranch.
2. Private line service to Mr. McNamara's residence from the White House switchboard has been rerouted.
3. Steps have been taken to design and fabricate transportable cryptographic communications equipment with reduced radiation levels which could accompany the President on trips, particularly abroad.
4. The C&P Telephone Company, in connection with certain new installations, is installing shielded cables direct from telephones in the West Wing to a consolidated terminal room now planned for construction.
5. White House police are now being taken to State for briefings in the audio surveillance threat and countermeasures.
6. The Secret Service has installed alarms in telephone terminal areas and other sensitive areas.
7. A better understanding of the technical penetration problems in the telephone companies has come about through very helpful discussions with representatives of AT&T, Chesapeake and Potomac, and Southwestern Bell, and those companies are considering development of technical features which would increase telephone security and privacy.
8. About 3,000 feet of surplus wire not needed for present service has been removed in the course of the special counter audio survey.

~~TOP SECRET~~

~~TOP SECRET~~

EXECUTIVE OFFICE OF THE PRESIDENT
BUREAU OF THE BUDGET
WASHINGTON, D.C. 20503

9

April 22, 1965

MEMORANDUM FOR GORDON CHASE

Subject: Additional Points Relating to Memorandum of April 21

1. The basic point is whatever the purpose of the installation in question, it could be carried out more effectively and with less risk by some other means. The basic requirement should be effective control over use by the proper person. WHCA, or whoever is asked to remedy the situation, should be given this control requirement as a basic premise.
2. WHCA's reply to our questions on this subject (copy attached) was very incomplete. We have not pressed them further on the matter. From this and other indications, it would appear that the installation was made subsequent to November, 1963, although we have no firm knowledge of this.
3. General Clifton was not aware of this particular problem and advised that the matter be taken up as proposed by Mr. Bundy.
4. Our examination was entirely technical. Initiative for any further investigation should come from the White House.
5. As far as the members of the special team and NSA are concerned, the condition was caused by a wiring mistake by WHCA. I have two technical reports on this matter - one by NSA and one by the special team. These will be made available to you on call.
6. Two parts of the technical investigation are continuing:
 - a. The instrument is being stripped down and examined by NSA.
 - b. We have initiated a complete mapping of wiring in the subject area to understand better its properties for conductance.

Attachment

JWC
JAMES W. CLARK

DECLASSIFIED

Authority NLJ-015-005-4-4-5
P: JC, NARA, Date 3-18-05

~~TOP SECRET~~

~~CONFIDENTIAL~~

9a

The KY-1 was initially installed in 1958. The only modifications have been to convert the whole net to full duplex (latter part 1958), change the telephone cover on the President's desk to a colored cover, and replace the first model secure voice switchboard with the second model (1960).

Ancillary equipment was installed in May 1962, removed in November 1962 and reinstalled in November 1962 by WHCA Technicians under instructions by WHCA Operations. No telephone company employees were involved.

The use of the KY-1 since initial installation has been infrequent. The line conditions are checked weekly by WHCA Technicians and is subject to PRS survey at anytime.

~~CONFIDENTIAL~~

DECLASSIFIED

Authority NJ-015-005-4-4-5

By pc, NARA, Date 3-18-05

PRESERVATION COPY

~~SECRET~~

GUIDE TO WHCA ASSESSMENT

APR 14 1965

98

1. When was the KYL installed initially?
2. What changes and modifications have been made in the installation (circuitry, switchboard, instrument, etc.) to date?
3. Recorder installation:
 - When was the recorder circuitry (including modification) installed?
 - Describe the initial installation and any changes thereto.
 - Who requested or authorized the installation initially, and who has authorized continuance?
 - Who in WHCA made the installation? Who checked and approved the installation?
 - What individuals in WHCA might have known about the nature of the installation?
4. Give names of all personnel (other than those in 4. above) involved in the operation and maintenance of the KYL installation and recorder.
5. Could telephone company employees have known about the installation and the resulting line conditions? If so, whom?
6. How often is the KYL used (give dates since the recorder was installed)? Indicate the number of times the recorder was used. What is the practice with respect to use of the recorder? What happens to the tapes?
7. Has the recorder ever been used for other than telephone conversations? How often is it tested? What happens to the tapes?
8. How frequently has the KYL line condition been checked since the recorder modification was installed? What reports have been made concerning it? What test methods were used?

DECLASSIFIED

Authority NLS-015-005-4-4-5
By je, NARA, Date 3-18-05

~~SECRET~~

To: McHally
4/14/65

~~SECRET~~
EYES ONLY

THE WHITE HOUSE
WASHINGTON

10

April 15, 1965

MEMORANDUM FOR MR. BUNDY

Attached is a list of the questions which Jim Clark is asking WHCA about the matter he reported to you on Wednesday morning. Jim expects to have a written report ready for you by Monday or Tuesday.

GC
Gordon Chase

DECLASSIFIED
E.O. 12356, Sec. 3.4(b)
White House Guidelines, Feb. 24, 1983
By Dett, NARA, Date 2-6-92

~~SECRET~~ - EYES ONLY

~~SECRET~~

GUIDE TO WHCA ASSESSMENT

Manding -

APR 14 1965

10a

1. When was the KYL installed initially?
2. What changes and modifications have been made in the installation (circuitry, switchboard, instrument, etc.) to date?
3. Recorder installation:
 - When was the recorder circuitry (including modification) installed?
 - Describe the initial installation and any changes thereto.
 - Who requested or authorized the installation initially, and who has authorized continuance?
 - Who in WHCA made the installation? Who checked and approved the installation?
 - What individuals in WHCA might have known about the nature of the installation?
4. Give names of all personnel (other than those in 4. above) involved in the operation and maintenance of the KYL installation and recorder.
5. Could telephone company employees have known about the installation and the resulting line conditions? If so, whom?
6. How often is the KYL used (give dates since the recorder was installed)? Indicate the number of times the recorder was used. What is the practice with respect to use of the recorder? What happens to the tapes?
7. Has the recorder ever been used for other than telephone conversations? How often is it tested? What happens to the tapes?
8. How frequently has the KYL line condition been checked since the recorder modification was installed? What reports have been made concerning it? What test methods were used?

DECLASSIFIED

Authority NLS-015-005-4-4-5

By jc NARA, Date 3-21-05

~~SECRET~~

~~SECRET~~

THE WHITE HOUSE
WASHINGTON

April 7, 1965

10:45

Chase

11

MEMORANDUM FOR MR. BUNDY ✓

SUBJECT: Communications Security

1. Attached is part of the draft Report which will be discussed at your meeting with Kermit Gordon on Thursday. ~~The balance of it will be here tonight or tomorrow morning.~~
2. Attendees at the meeting will be you, Kermit, Don Hornig, Jim Clark and his study group, and me.
3. The meeting will probably involve a briefing on the work of the Study Group and a review of the draft Report. In view of the fact that the Report is not yet in final form, Kermit will probably be especially interested in your reactions -- e.g., From a White House view, do any of the recommendations seem silly? Which points seem most significant? What is the best approach to take in presenting the Report?

GC
Gordon Chase



DECLASSIFIED

E.O. 12356, Sec. 3.4(b)

White House Guidelines, Feb. 24, 1983

By DA, NARA, Date 2-6-91

SECRET

M-5B/65-S/11 Cy. 4

Mr Bundy

1422

12

DRAFT REPORT

SURVEY OF TECHNICAL
AND PHYSICAL SECURITY ARRANGEMENTS
FOR THE PRESIDENCY

SANITIZED

E.O. 13526, Sec. 3.5

NLJ/RAC 05-47

By isl NARA, Date 12-6-11

E.O. 12958

3.3 (b)(1)(7)

NSAM 315 Steering Group

April 7, 1965

TABLE OF CONTENTS

	<u>Page</u>
I. Objectives and Approach of the Survey -----	1
II. Summary of Major Conclusions and Recommendations -----	4
General Security and Audio Surveillance Countermeasures ---	5
Recommendations	9
Telephones and Communications -----	11
Recommendations -----	15
III. Discussion of General Security and Audio Countermeasures -----	17
Background -----	17
Physical and Personnel Security -----	18
Technical Security -----	22
Classified Document Handling -----	26
IV. Discussion of Telephones and Communications -----	29
Need for a New System -----	29
Evaluation of Security of White House Telephone Facilities ----	32
Responsibility for Protection of Telephone Systems -----	34
Crypto-Secure Telephones -----	36
Communications at the LBJ Ranch -----	36
Compromising Radiations (TEMPEST) -----	37
White House Office Machines -----	39

~~SECRET~~

M-5B/65-8/11

April 7, 1965

SURVEY OF TECHNICAL AND PHYSICAL SECURITY ARRANGEMENTS
FOR THE PRESIDENCY

I. OBJECTIVES AND APPROACH OF THE SURVEY

The survey, in response to National Security Action Memorandum 315, has the following general objectives:

- To assess the present program for protecting the privacy and security of the Presidency in terms of current capabilities for technical penetration.
- To assess for the President and his advisers the risks of compromise involved in the use of various communications and other facilities.
- To recommend specific measures to reduce risks, which are realistic in terms of cost and the needs and functions of the White House.
- To recommend arrangements for a sound and continuing technical protection program paced to the growing risks which would minimize the possibilities of compromise or embarrassment to the Presidency.
- To assess the handling of classified documents in the White House, especially certain highly sensitive documents sent to the President.

To conduct the survey, the Director of the Bureau of the Budget convened a committee of experienced officials from CIA, NSA, State, and Defense, and representatives of the Executive Office (listed on Attachment A), hereafter referred to as the Steering Group. These men were selected to provide a balanced expertise in intelligence and security from both an operational and research and development viewpoint. In addition, the survey and the

~~SECRET~~

~~SECRET~~

2

conclusions have been reviewed by a panel of scientific and engineering consultants consisting of Dr. Jerome B. Wiesner, Dr. William O. Baker, Dr. Edward David, and Mr. Richard James (see Attachment A).

In the course of the survey, it was determined that conditions in two areas required more detailed and comprehensive inspections, and these were initiated:

- Defense was requested to investigate possible compromising radiations from equipment utilized for secure or encrypted communications. A team of Army specialists, supported by NSA, conducted this inspection (known as TEMPEST) at the White House and the ranch in Texas. The results of this survey are set forth in Appendix ____.
- Secret Service was requested to conduct an intensive audio counter-measures survey of the White House. The Secret Service personnel normally involved in such surveys were augmented for this effort with equipment and highly trained personnel from State, Defense, and CIA. This work is still in progress.

The report concentrates on security protection at the White House but also touches upon relevant situations at the President's ranch in Texas, at the office in Austin, Texas, and while he is travelling. The problems of the Executive Office Building (EOB) and, to a lesser extent, the new Federal Office Building No. 7 are treated as they relate to White House problems.

~~SECRET~~

~~SECRET~~

3

The emphasis of the survey has been placed upon technical security, i.e., (a) protection against hostile audio surveillance (clandestine microphones and transmitters, compromised or "hot" telephones which are activated even when on the hook, telephone taps, and so-called sophisticated "remote" listening techniques like infra-red windowpane pick-off), and (b) protection against surveillance of compromising radiations from communications equipments (TEMPEST). However, it was clear from the start that technical security programs had to be viewed as a part of a total security effort which would include the classical elements of physical and personnel security such as perimeter protection, personnel clearances, passes, and access control. These elements are treated in the report primarily as they pertain to the central mission of technical security.

For the detailed aspects of the survey, the participants were organized into two panels. The first panel, chaired by [REDACTED] CIA, assessed the audio countermeasures and related physical and personnel security aspects of the problem. The second panel, chaired by Leo Rosen of NSA, focused on various aspects of communications security.

In the conduct of the study, the Group was hampered somewhat by the fact that there is no central authority on security procedures in the White House. It was, therefore, necessary to obtain information from a number of sources, and such information often proved conflicting. In addition, certain procedures, such as security clearances and issuance of White House

~~SECRET~~

~~SECRET~~

4

passes, were revised during the course of the study. Also, since the survey began, basic changes have been initiated in the telephone system.

The comprehensive reports and specific recommendations of the Steering Group are attached as annexes, tabbed as follows:

- A. AUDIO COUNTERMEASURES PROTECTION
- B. CLASSIFIED DOCUMENTS CONTROL
- C. PHYSICAL SECURITY IN THE WHITE HOUSE
- D. PERSONNEL SECURITY CLEARANCES
- E. COMMUNICATIONS AND TELEPHONE SECURITY
- F. LBJ RANCH AND THE AUSTIN OFFICE

II. SUMMARY OF MAJOR CONCLUSIONS AND RECOMMENDATIONS

The growing importance of the Presidency on the national and international scenes and the increasing flow of information to, from, and within the White House have necessarily increased its attractiveness as an intelligence target. This trend has been paralleled by a marked and continuing expansion in technical capabilities for clandestine eavesdropping by intelligence agencies and by news, business, and political groups. The Soviets in particular have demonstrated high proficiency in this area, as evidenced in the operations against the U. S. Embassy in Moscow since 1952. Domestically, eavesdropping devices are widely and increasingly available on the commercial market, and a growing number of private detective agencies stand ready to provide such services. In the next five years, intensive

~~SECRET~~

~~SECRET~~

5

application of microelectronics and other developments now in the laboratories can be expected to increase significantly the use of clandestine surveillance systems and the difficulty in countering them effectively.

The principal conclusions and recommendations resulting from the survey are summarized below under two headings: (1) General Security and Audio Surveillance Countermeasures, and (2) Telephones and Communications.

General Security and Audio Surveillance Countermeasures

Given the importance of the office and the motivations and capabilities of potential penetrators, the Presidency deserves extraordinary precautions to protect privacy and security using the best personnel, equipment, and techniques available. In contrast, the actual audio surveillance countermeasures program at the White House has developed with little guidance and support and, as a consequence, is mediocre in terms of what could be done.

Fundamentally contributing to this condition is the fact that there is no comprehensive security program in the White House in the sense of providing protection to national defense information, either communicated electronically spoken, or written. There are fragmentary security functions, but there is no central authority within the White House to direct and integrate them as a meaningful whole. Security files for White House personnel are reviewed by Mr. Watson; Mr. Moyers has responsibility for approving pass issuance and for communications; Mr. Bundy controls the handling of most classified documents; Secret Service with the White House

~~SECRET~~

~~SECRET~~

6

Police provides certain physical security; Secret Service exercises responsibility for audio countermeasures for most of the White House and security pertaining to administrative (non-military) communications; the White House Communications Agency (WHCA) provides security for its communications; and the FBI performs full field investigations and specific counter audio and communications investigations on call.

This diffusion of responsibility has resulted in gaps in the overall effectiveness of the White House security program. It certainly is not conducive to developing a program to meet the increasing technical threat.

There has been a tendency in the past to assume that Secret Service and White House Police functions provide adequately for the protection of defense information (hereafter referred to as security), and, in fact, a considerable measure of security has resulted from efforts to protect the person of the President and the White House premises. However, there is no statutory authority or written directive assigning Secret Service any responsibilities for technical and physical security per se. It is not surprising then that the orientation and competence of the Secret Service continue to lie in its traditional areas of protection and investigation and that security coverage is not complete.

There are good reasons for having the Secret Service provide an "in-house" audio surveillance countermeasures program as many of these functions can be fitted in most easily with other activities related to protection of

~~SECRET~~

~~SECRET~~

7

the President and the White House. However, the basic unknown is whether the Secret Service management can give proper support and direction to the technical security functions and whether a "police" agency can attract, retain, and direct the technical competence required for the handling of the more sophisticated audio threat anticipated in the next few years. It is especially important that the director of the technical security program be highly qualified in engineering or the physical sciences. If Secret Service is not able to hire such a person directly, consideration should be given to providing such a person on a two - three year rotational basis from the intelligence community.

We conclude that the Secret Service can and should develop an effective countermeasures program, if the recommendations herein for strengthening its capabilities in this field are implemented. The alternatives of assigning responsibility for this function (a) to WHCA, (b) to a new civil service unit attached to the White House or some office in the Executive Office of the President, or (c) to an operating agency like State, Defense, or CIA were considered and rejected as less desirable. If it appears, however, that after a year the Secret Service program has not developed the technical leadership and competence required, alternative arrangements should be reconsidered.

Four other conclusions are worthy of note. First, based upon discussions with personnel involved with various aspects of White House security, there has been no concrete evidence of audio surveillance activities

~~SECRET~~

~~SECRET~~

8

directed against the Presidency in this country. None has been uncovered in the comprehensive counter audio survey to date. Even after the completion of the comprehensive survey, it should not be interpreted as 100 percent assurance that the White House is free of audio surveillance devices.

Second, the major problem in providing technical protection is considered to be control of people who have access to sensitive spaces and who may have been induced to cooperate with intelligence or other groups in effecting a technical penetration. In the White House, there are thousands of people who enter sensitive spaces each year, including visitors, guests, military support personnel, maintenance personnel, tradesmen, and members of the news media. For example, there are the 4 - 5,000 telephone maintenance men, construction and repair workmen, TV technicians, vendors, etc., entering the White House each year, who do not receive the clearances given regular White House personnel.

Consideration was given to the usefulness in the White House of special protective features used by sensitive agencies overseas, such as secure rooms, plugs in jacks for telephones, hushaphones, and background masking noises. It was concluded, however, that because of the operational inconvenience and the "image" that might be conveyed, such devices would not be acceptable to the White House.

~~SECRET~~

~~SECRET~~

9

Lastly, given the lack of overall security procedures, the basic, informal system centered in Mr. Bundy's office for handling and controlling classified documents in the White House is reasonably effective. Improvements could, however, be made by attempting to reduce the number of people handling classified documents in the President's night reading file, as described below.

Principal recommendations with respect to the general White House security and audio countermeasures are:

1. Responsibility for physical security, telephone security, audio countermeasures, and personnel clearances should be clearly assigned to a single Presidential assistant. Responsibility for classified document control could be treated separately, as at present, but under the general cognizance of the proposed Security Officer.

2. Staff support for the designated Presidential assistant should be provided by a professional, high-grade security officer reporting directly to such assistant and responsible for ensuring that a comprehensive security program is established, appropriately coordinated, and effectively maintained.

3. Responsibility for the audio countermeasures program in the White House and at residences of key Presidential staff should be assigned to the Secret Service, and execution should be carefully monitored and coordinated by the White House Security

~~SECRET~~

~~SECRET~~

10

Officer. The intelligence community should provide staff and equipment to supplement that of the Secret Service on request from the White House. If necessary, a highly qualified technical director for the program should be supplied from the community. Also, the technical security function should be separated from the Protective Research Section and given greater status within the Secret Service organization.

4. The Secret Service countermeasures program should be reviewed in a year by a committee chaired by the Director, Office of Science and Technology, to insure that progress is being made toward developing an effective program in terms of the threat.

5. The charter of the Technical Surveillance Countermeasures Committee of the U. S. Intelligence Board should be amended to ensure that this Committee gives adequate attention to technical or operational problems at the White House. Secret Service should be made a permanent member of the Committee.

6. Staff of the Secret Service performing the technical security function should be increased by at least five people. All should be technically trained, and at least two of them graduate engineers. The frequency and coverage of the audio countermeasures program should be extended and intensified as recommended in Appendix A, pages ____ to ____.

~~SECRET~~

~~SECRET~~

11

Telephones and Communications

Communications are a vital instrument of Presidential command, and effective communications, starting with the systems closest to the President, deserve high national priority. Important attributes of an effective system are privacy and security. All men deserve privacy in communications, but the President of the United States requires the best protection possible.

The telephone security problem at the White House is inherent in the system. The basic system serving the White House is old and fast reaching its capacity. It does not provide an adequate base for future system development, and it certainly was not designed with security in mind. In this light, it would make sense to develop a new backbone system than to continue to tinker piecemeal with the present system. This appears to be an appropriate time to consider a new telephone system with desirable security features, in view of possible renovations in the Executive Office Building and the construction status of the new Federal Office Building No. 7. If decisions to plan the telephone complex are taken immediately, it will probably be 18 - 24 months before a new system could be implemented.

As in the general security area, there is no clear responsibility for planning communications in the White House, particularly technical planning. No single person is responsible for integrating Presidential and White House staff needs in day-to-day and emergency situations and seeing that appropriate plans are developed to meet them. It is believed that communications are so important to the President that general responsibility should be placed in one Presidential assistant. This assistant, however, must be given strong technical support.

~~SECRET~~

~~SECRET~~
~~SECRET~~

12

The most logical official to turn to for technical support is the Director of Telecommunications Management (DTM), who already performs a number of communications functions for the President, including the development of Presidential requirements for inclusion in technical planning for the National Communications System (NCS). With a small staff of competent engineers, the DTM could work with the telephone companies, the Defense Communications Agency, GSA, and others to see that longer term system capabilities provided the President are modern, secure, and adequate to his informational and command needs.

For historical and practical reasons, there is a split responsibility for providing day-to-day operational communications support to the White House. The so-called administrative or White House switchboard, manned by civilian operators under the direction of the White House Clerk, provides an estimated 90 percent of the total telephone volume at the White House. WHCA provides the balance of the White House service from the "signal" switchboard in the East Wing shelter area and, in addition, is responsible for secure communications, emergency communications, and all communications for the President at the ranch and in travel.

(Private telephone companies install and maintain almost all the equipment used by both groups.) This split also extends to security responsibilities. Secret Service is nominally responsible for the communications provided through the administrative switchboard, and WHCA is responsible for security of its communications.

~~SECRET~~
~~SECRET~~

(SECRET)

The White House will need to be served by a combination of WHCA and civilian-operated communications. However, the present diversity of facilities and responsibilities does not appear to represent the most rational pattern. Before new systems are planned and implemented, there is a great need to review these relationships to determine an optimum balance, especially as more crypto secure communications are introduced.

In any case, guidance for WHCA should come directly from the designated Presidential assistant. Such guidance is not now being received, and the effectiveness of this very vital element of Presidential support is weakened because of it.

There is a tendency for some to assume that the private line services from the White House switchboards to offices and residences provide a measure of security above that of regular dial service. In fact, the opposite is true. The private line circuits outside the White House and EOB pass through telephone exchanges (usually two or three) where they are "tagged" for special service. In the exchanges, they may be monitored by maintenance people, even more frequently than other lines, to ensure quality and reliability. Most vulnerable to tapping is the segment from the last telephone office to the home, especially where it goes into overhead wire. Many of these lines "appear" individually several times (eight times for Secretary Rusk), and these appearances make easy tapping points. As an example, Secretary McNamara's private line was found to run along the back wall of the Finnish Embassy. (This has been since remedied.)

(SECRET)

We conclude that it would be almost impossible to afford any realistic degree of protection to these private lines.

On several occasions, questions have been raised as to the relationship between audible clicks on telephone lines and possible tapping. Based upon a study by the Chesapeake and Potomac Telephone Company, the greatest source of clicks is the operator checking the line to see if calls are completed. Clicks also result from maintenance people checking lines and very infrequently from natural phenomena. A telephone tap generally cannot be detected audibly. In fact, there is no certain electrical means for determining whether telephone lines are being tapped. Physical inspection of the circuit remains the best method of detection, and, given a resourceful tapper, this is difficult.

The greatest risk of interception relates to the mobile radio telephones in cars, helicopters, and aircraft. The frequencies used are widely known, and, in the Washington area, it must be assumed that these are monitored in the Russian Embassy and in other places. The radio telephone system at the ranch is also susceptible to intercept over a 50-mile radius by agents, newsmen, or anyone else willing to invest in a receiver. Radio telephones of aircraft, especially those carrying the President, are monitored in many places.

~~SECRET~~

15

Principal recommendations with respect to telephones and communications are:

1. Responsibility for Presidential communications should be placed clearly on a Presidential assistant, preferably the same person having general security responsibility.
2. On technical matters, such as the planning for facilities, capabilities, and security, the designated special assistant should look to the DTM for support. The DTM should acquire the necessary technical competence to perform this task.
3. The designated assistant for communications should request the DTM to work with the telephone company, WHCA, Defense, GSA, and the White House Chief Clerk to develop and recommend a rational telephone system for the White House - EOB complex, with the following security features:
 - a. A self-contained system serving the whole White House - EOB complex and physically secured;
 - b. A combination of manual operation and a flexible dial system so that calls can be made without going through the operator.
 - c. An automatic disconnect capability, even for the dial portion, so that when the inside telephone is hung up, the line into the White House does not remain open to outsiders.
 - d. Some form of operator disconnect on calls that have been established so that the operator cannot re-enter the circuit except on recall by the parties.
 - e. Maximum cryptographic security for links outside the complex.

~~SECRET~~

~~SECRET~~

16

4. New and improved secure telephones (KY3 and FY8) should be installed to connect the President and key officials in their offices and homes as soon as the system is fully engineered.

5. Under the guidance of the proposed White House Security Officer, the Secret Service should be responsible for protection of all White House telephones which are not cryptographically secure. The Secret Service may seek technical assistance of the DTM as required. WHCA should provide security for its communication systems.

6. Supervision and guidance to WHCA should be provided by the designated Presidential assistant.

7. Until secure phones are available, the Secret Service should check the private line service to key residences of White House officials through the exchanges and from the last exchange to the residence in order to identify and to have corrected obviously insecure conditions.

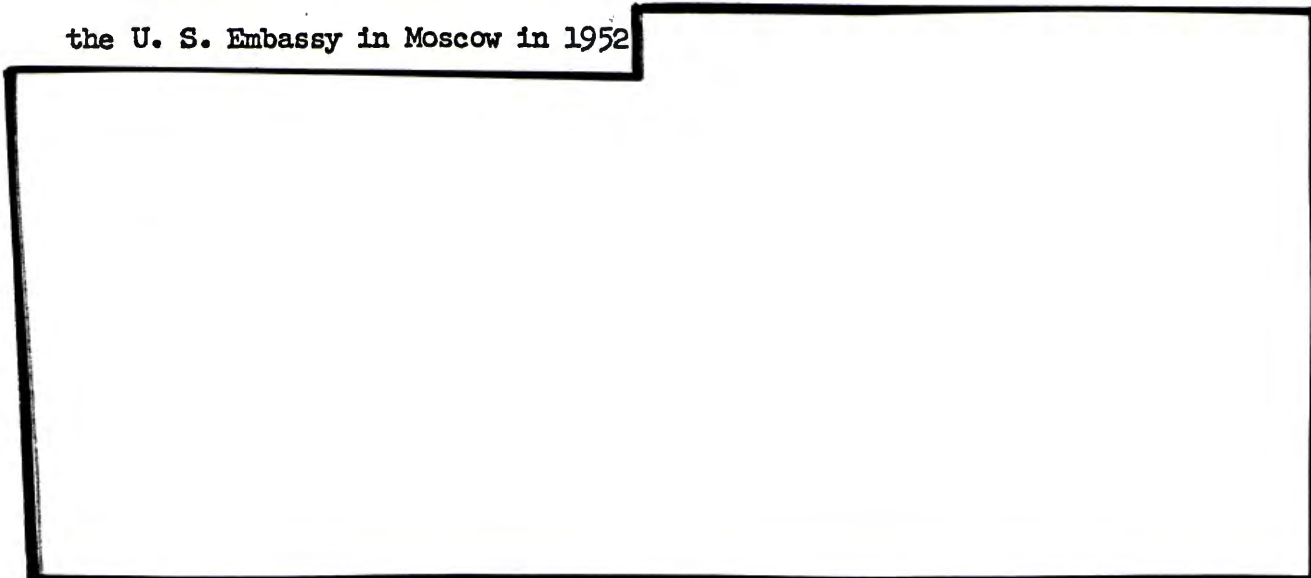
8. In any case, key staff of NSC supporting Mr. Bundy should be served by the White House board, rather than through existing EOB terminals and the downtown exchange.

~~SECRET~~


III. DISCUSSION OF GENERAL SECURITY AND AUDIO COUNTERMEASURES

A. Background

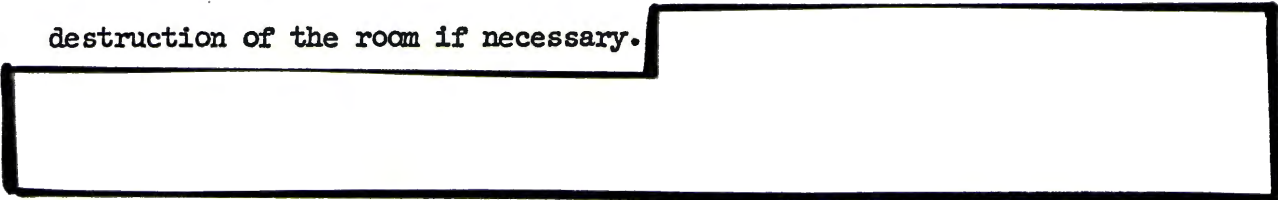
The Soviets (and other foreign powers) have given considerable emphasis to the development of audio surveillance techniques. Soviet proficiency in this area is evidenced by the cavity resonator in the Great Seal in the U. S. Embassy in Moscow in 1952



Since 1949, over 750 hostile audio surveillance devices have been targeted against U. S. and allied facilities abroad, about 350 of which were against the U. S. It is also known that industrial intelligence collection is widespread within the U. S. and includes telephone tapping and microphone and radio transmitter installations.

Technical defense against audio surveillance is behind "the offense." A DIA-CIA panel of experts indicated its concern at the lack of counter-measure sophistication and recommended increased attention to development of improved  Notably, there is no operational equipment to detect buried microphones, and the most effective

method of discovery is extensive physical inspection, including complete destruction of the room if necessary.

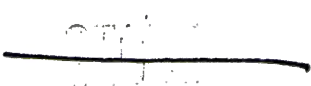


B. Physical and Personnel Security

In assessing the effectiveness of counter audio surveillance protection at the White House, it was necessary first to review the current physical and personnel security measures in the White House and to note basic conditions at the White House which affect technical protection capabilities.

As to the physical security aspects, the White House, located on an open plot of ground, is relatively isolated from other buildings, particularly non-Government controlled buildings. These spatial factors tend to pose more difficult problems for transmission of information out of the White House to areas which contain potential listening posts. For example, the greater distances tend to increase the power required for radio transmitters or to necessitate relay points, both of which increase the possibilities for detection.

The present physical security program of the Secret Service, established primarily for the personal protection of the President, does provide a measure of protection against penetrations. However, the present perimeter lighting and perimeter alarm systems are not considered adequate given the large amount of masking foliage on the White House grounds.



~~SECRET~~

19

Moreover, it is believed advisable to provide additional protection during non-working hours through the use of alarms on ground level windows and doors not manned by White House Police. (See Appendix ____.)

A basic problem is to control the movements of people in a facility where rapid action is the rule. White House Police statistics show the following numbers of people moving through the White House in FY 1964, in addition to the professional and secretarial staff, domestic help, messengers, char forces, gardeners, and agency officials having White House passes:

- 4 - 5,000 Tradesmen, vendors, construction and contractor personnel, including TV and radio technicians service the White House in a year, many returning a number of times (25,700 separate entries)
- 51,500 Guests at social functions
- 1,840,000 Public visitors and tourists
- 49,000 Official visitors
- 2,000 Military people supporting the White House, including communications personnel, mess stewards, chauffeurs and bands
- 1,700 Members of the press, TV, and radio

In terms of the study, the construction maintenance workmen (including electricians), telephone maintenance men, and TV technicians are of particular interest. For example, there were seven different contractors

~~SECRET~~

and 90 workmen in the West Wing and the Mansion on a recent week-end, and this is considered a typical level of activity. The fast pace and pressures of White House activity make surveillance of these types of people difficult. A quick decision to have TV coverage of an event can result in 40 - 50 technicians setting up lights and cameras and running cable in the President's office and adjacent areas for a period of several hours. In this frenzy, it is not easy for the Secret Service or White House Police to maintain careful surveillance. TV coverage is liable to be followed almost immediately by a high-level meeting in the President's office with no time in between to conduct a countermeasures search.

The system of controlling this total movement of personnel should be improved as follows: (1) White House passes should be revised, re-issued, and more tightly controlled; (2) the escort system recently established in the West Wing should be closely adhered to and extended to the East Wing; and (3) more effective controls and surveillance of movement of press, TV, maintenance and trades people should be exercised within sensitive areas. (See Appendix ____.)

A basic deficiency in the present security system is the lack of a central authority controlling construction, renovation, etc., and regular procedures for coordinating changes in physical plant in advance with Secret Service. (This results in part from the fact that basic responsibilities for construction are spread between GSA for the East and West Wings; National Park

Service for the Mansion; and Navy for the shelter area.) It is not an infrequent occurrence that the first Secret Service hears of a project is the daily notice that contractor employees will arrive on the job.

Lastly, the White House is an old facility to which features have been added piecemeal. Space and other aspects of the plant have been altered many times, and, in many instances, up-to-date engineering drawings are not available. Telephone, electrical and other wiring and piping particularly have been added over the years without any systematic effort to remove the old.

As to the personnel security, in the last few months, clearer and more effective procedures for reviewing FBI investigations and approving assignments to White House staff have been established. However, the many other systems for clearing and admitting people to the White House (described in Appendix ____) should also be reviewed.

Secret Service investigates and clears its own personnel and grants passes to maintenance employees of GSA and the National Park Service on the basis of review of files furnished by those agencies. Secret Service also makes very limited checks on tradesmen and contract personnel. These personnel are difficult to check, especially if contractors hire people on a daily basis from union halls. Before issuing permanent passes, members of the news media are checked through criminal files of the FBI and police records, and, if the person has foreign connections, CIA files

are checked. Telephone maintenance men possessing White House passes are not given full field investigations by FBI, but are investigated by Military District of Washington, U. S. Army, at the request of the local telephone company. Secret Service issues a pass on the basis of certification of clearance with no further review of the files. Military personnel are investigated by their Service, and the files are reviewed by DOD, a Presidential assistant, and the Secret Service. However, the formality of granting a security clearance is left to many commands, and practices vary.

It is believed that all people permanently assigned to the White House (except Secret Service and military personnel) should receive full field investigations by the FBI, Secret Service, and military services, as appropriate. The approved investigation reports should constitute authority for access to Top Secret material as required. Authority for issuance of a White House pass should be placed in the person who has the basic security responsibility.

C. Technical Security

Given the general security arrangements at the White House and its distance from potential listening posts, the most likely form of technical penetration is the small, self-powered radio transmitter which could be concealed quickly by someone having limited access, like construction and repair workmen, vendors, TV technicians, press, etc. Other forms of penetration like concealment of a miniature recorder (cigarette package

~~SECRET~~

(~~SECRET~~)

size), microphones or carrier transmitters using existing wiring in the White House, or telephone compromises cannot be ruled out. Sophisticated penetration techniques, such as infra-red windowpane pick-off, lasers, etc., are presently limited by operational conditions and the state of the art, but must be considered in developing future protection programs.

(See Appendix ____, page ____.)

The Secret Service program to protect the President from technical eavesdropping began in the early phases of World War II. The protection of Presidential privacy was considered a logical extension of the statutory responsibility "to protect the person of the President" and his immediate family. As late as 1962, there were only two people concerned with audio countermeasures. In the last year, the number has been increased to six, although only about 50 percent of the time of these men is spent on audio countermeasures per se.

From time to time, Secret Service has used manpower from other agencies to perform counter audio "sweeps." The most frequent assistance was received from WHCA and Army security units. On occasions, when new technical dimensions of the threat were uncovered, like the discovery of the cavity resonator in Moscow, the FBI was requested to conduct a special search. To this day, the efforts of the Secret Service are supplemented by WHCA on trips in the U. S. and by State and Defense on trips abroad.

(~~SECRET~~)

In the absence of guidance and continuing supervision from above (either the White House or the Treasury), it is not surprising that the Secret Service management has not allocated scarce budgetary and manpower resources to the countermeasures effort. The program has tended to drift along, and one senses that a major objective has been to conduct the program in such a way that it does not "bother" the President and staff. Appendix A contains a detailed review of the program and 16 recommendations for improvement. In general, the situation found can be summarized as follows:

- Inspections are cursory and too infrequent given the threat and high usage of the sensitive space by uncleared and uncontrolled people.
- There are important gaps in coverage; e.g., the offices of the NSC staff are not given counter audio protection, nor are the residences of key White House aides.
- There are not sufficient qualified technical people conducting the program.

Increasingly in the future, the detection of sophisticated types of threat, such as transmitters whose transmission patterns blend with background "noise," will require professional engineering personnel. The Secret Service should not rely on promotion from the investigative elements of the Service for recruitment for this program. The Service should make increasing use of the schools of the intelligence community for this training.

A question arises as to whether the Secret Service is the appropriate agency to conduct the audio countermeasures program in the future. Many activities have to be done on a daily basis - such as RF monitoring during sensitive meetings, quick searches after use of the President's office by TV crews, and morning checks of the President's office. These can be fitted in most easily with other Secret Service activities related to the protection of the President and the White House.

A basic unknown is whether a "police" agency can attract, retain, and direct the technical competence required for handling the more sophisticated audio surveillance threat anticipated in the next few years. Secret Service has experienced some difficulty in recruiting such competence in the past and may continue to have difficulty in the future. The only engineer is reported to have tendered his resignation.

However, we see no better alternative to Secret Service. WHCA has technically trained people, but a strong communications bias. Its present program does not appear any more effective than that of Secret Service. Use of agencies like Defense, State, CIA, and FBI, for the whole audio countermeasures job would add another party to the White House routine which would fragment further the already splintered security responsibility, increase the number of people operating in a crowded facility, and increase the already complicated problems of preparing for Presidential trips. A

third alternative to Secret Service would be a professional technical security staff assigned (a) to the White House, or (b) more realistically to some element of the Executive Office of the President, such as the Office of the Director of Telecommunications Management. This approach would separate this function from the protection and investigative orientation of the Secret Service, and perhaps the civil service system would facilitate the hiring of competent engineers and technicians. However, this would mean adding about 10 people to the rolls of some office in the Executive Office complex.

It is concluded that, since Secret Service already has large aspects of the task protecting the President and the White House, it makes sense for them to continue the technical security function. However, we believe that the program will be successful only if Secret Service management recruits a top-quality person with strong technical background to head the program (if necessary, by borrowing from intelligence agencies) and separates the counter audio functions from the rest of protective research.

D. Classified Document Handling

By far, the larger percentage of total volume of written material received and handled within the White House is unclassified, although much of it is sensitive. It is the accepted premise that anything addressed to the President is automatically "Confidential" and "Personal" in nature, and this premise undergirds the system for handling formally classified documents.

~~SECRET~~

27

The survey revealed that there are no written procedures, now in effect for handling classified documents in the White House. However, a less formal system has evolved, centered primarily on Mr. Bundy's operation, which appears remarkably effective considering the unique situation of the White House, the pace at which papers are handled, and the lack of any overall security authority noted above. Although the committee was informed of lapses which have occurred in the past, the people with whom the problem was discussed exhibited a reasonable and consistent understanding of the present system and an excellent awareness of the need to protect documents.

The informal system has worked largely because of (a) close attention given the system within the Bundy-NSC complex, (b) the high quality of the staff in this area who keep track of documents and administer the system, (c) the willingness of staffs in other key areas to use the document-handling services provided by the Bundy complex, and (d) the general good sense and ability of White House personnel, especially the secretaries, in handling carefully all sensitive papers, classified and unclassified.

We have reviewed with special care the handling of the highly classified material which becomes a part of the President's "night reading" file, particularly the State Department's "Evening Reading" and CIA's "President's Daily Brief," the latter containing COMINT and other highly sensitive material. It is concluded that, although these materials appear to be

~~SECRET~~

handled with awareness and sensitivity by all concerned, the security of the process would be improved by reducing the number of people who handle or have access to these materials on the way to the President. For example, these materials, generally received in Mr. Bundy's office between 6:30 and 7:00 P.M. each evening, are forwarded to the President's secretary for inclusion in the night reading file, delivered by a White House messenger to the Head Usher, handed to the Doorman, who either gives them to the Sergeant valets on duty or takes them directly to the President's private quarters. If the President is out for the evening, the documents remain untended on his bed until his return to the White House. A preferable way to handle these documents might be to hold them in the Situation Room and to have the watch officer deliver the documents to the President's quarters when notified that he has returned.

With respect to organizational responsibilities, it is clear that the President's Assistant for National Security Affairs will, by the very nature of his task, have to handle the vast majority of classified documents, especially those involving special categories of clearances. It was indicated that about 95 percent of classified documents flow into or through the Bundy complex. It, thus, makes sense to concentrate the handling of such paper in his office, backed by the NSC staff, as is now the case. However, overall responsibility for ensuring that there is a system, that it fits adequately with the rest of the physical security program, and that it is adequately understood, especially by secretaries and administrative assistants in other offices, should be exercised by

the designated Special Assistant for Security and the proposed White House Security Officer.

An example of the type of problem requiring attention is that of securing classified documents after hours. The committee was advised that responsibility for securing classified documents at the close of the day resides in each office and that each office organizes its own checks on performance. However, it is not uncommon that classified materials, including Top Secret, are left on desks, in piles of paper, or in desk drawers. Evidence of this was observed by the committee. It is the committee's view that the present physical security system administered by the White House Police and Secret Service is not designed for and provides inadequate protection for classified material.

IV. DISCUSSION OF TELEPHONES AND COMMUNICATIONS

Need for a New System

From a security point of view, the present telephone system at the White House was unplanned, and grew like Topsy. Frequent changes accomplished under tight time pressures have resulted in the following basic conditions:

- The three manual switchboards for this facility not only add to system complexity but increase the number of operators who can overhear telephone conversations.
- There are too many terminal boards serving the White House, and they are inadequately secured (being corrected since the study began).

~~SECRET~~

- Cables are old and vulnerable to "cross-talk." This has been a frequent problem in the past.
- There is an extraordinary amount of unused wire and equipment which might be used in a penetration and makes inspection difficult.
- The records of the White House telephone service were inadequate at the outset of the study making it difficult for anyone to check security of the system.

The White House system is extensive, providing a wide variety of services, including regular telephone service through three switchboards (White House, "Signal" and police boards), cryptographically secure voice and teletype systems, separate press and TV services, closed circuit TV, alarm systems, etc. There are about:

- 270 lines off the White House switchboard, including 23 to private residences.
- 555 lines off the Signal Board, including 111 to private residences.
- 56 lines off the Police Board.

In all, there are about 895 telephone instruments, of which about 60 percent are in the West Wing.

WHCA "Signal" switchboard has already reached its capacity, and the White House switchboard at the present rate of growth in service is expected to reach saturation next year. Ever since the White House board was moved to the EOB in 1962, the system has been considered "interim" by the Chesapeake and Potomac Telephone Company. The Company has been awaiting

~~SECRET~~

a decision from the White House to develop an improved system. There have been many technical improvements since the White House switchboard was designed, and many of these have been incorporated in facilities available to other agencies.

Because of the importance of the President's telephone system to his command and executive functions, these systems in the future should not be left to chance and evolution. It is strongly in the nation's interest to see that the President has an effectively planned communications system with the best features of privacy and security built into it from the beginning.

Basic questions with respect to a new system are (a) whether it should be self-contained (electronically segregated and physically secured), and (b) how much of the Executive Office of the President it should embrace. It would appear that the long-run trend will be to move more activities directly supporting the White House into the EOB and Federal Office Building (FOB) No. 7. It would appear prudent at this time to consider the White House - EOB - FOB No. 7 as a single complex served from a central switchboard in the EOB. This switchboard could have dual capabilities - a manual capability serving the President and top staff as determined by later studies, and a flexible, rapid dial system which could ring anyone in the complex by dialing only two or three digits.

This single system should largely replace the three switchboards now in use with considerable savings in the number of operators, trunking, and line costs. In fact, the C&P Telephone Company has estimated that such new service could be rendered for approximately the same annual recurring cost as that for the present system. In the system studies which are required, these cost factors should be carefully weighed.

It is significant to note that the present GSA plans call for telephone service to both EOB (with exception of certain lines from the White House board) and FOB No. 7 to be furnished from the main Government (Lafayette) exchange also through a modern dial service. This, however, would mean that calls from the EOB to the White House would go out through main feeder cables to the exchange and back to the White House board and thus be available to intercept in the exchange and cables.

Evaluation of Security of Telephone Facilities

The present White House telephone system (and in fact the basic domestic telephone service) was not designed with security as a major objective. There are many techniques of tapping the telephones which can be so disguised that they are very difficult to detect, even by trained people. Even pressurized and alarmed cables can be opened and tapped by experts without triggering the alarm. Thus, all telephones out of the White House, except those which are cryptographically secure, must be considered basically unsecure. In this connection the familiar weapon of "double talk" does little to confuse an intelligence analyst once the conversation

~~SECRET~~

has been intercepted.

The most vulnerable elements of the White House telephone system are summarized below, from the greatest to the least risk:

- a. Mobile telephones to cars, helicopters, and aircraft;
- b. Private lines outside the White House which are vulnerable both in exchanges and in the portion from the last section to the residence or office;
- c. The EOB telephone system served from the Lafayette exchange;
- d. The main "feeder" cables from the White House to the downtown exchange;
- e. The internal White House telephone system, especially the terminal room for Presidential and White House communications in room 578 of the EOB.

Vulnerability of these elements are assessed in greater detail in the Appendix, pages ____ to _____. However, certain points deserve emphasis here:

1. The EOB has less security (control of visitors, etc.) than the White House, and up to two years ago was a completely open facility. Moreover, the terminal board in the basement (room 045) serving the EOB is so cluttered with old wires that a tap would be very difficult to detect. It is noted that this board serves many sensitive offices, including NSC staff supporting Mr. Bundy. To reach Mr. Bundy, for example, calls from these offices must also go through the downtown exchange and back to the White House board in the EOB.

~~SECRET~~

2. The two large underground telephone "feeder" cables in and out of the White House both run to the same downtown exchange over different paths. The only inspection is by telephone people, where the cable appears in manholes and when there is trouble which is infrequent. A tunnelling to the cable of the type accomplished by U. S. intelligence groups in East Berlin would be difficult to accomplish, but also extremely difficult to detect.

3. In the basement of the West Wing is a recording studio operated by WHCA. About 75 telephone circuits run from the main West Wing terminal (the Bulb Room) to the studio, giving it a capability of recording or listening to telephone conversations of the President and key White House staff members after making a simple "patch" requiring about one minute. This can be done without the knowledge of the parties involved.

4. Speaker phones are available in the offices of the President and several of his top aides, and it is understood that they are extensively used. It is also understood that, between calls, the speaker phones in the President's office are held on "intercom," which means that they are "open" to room conversations. These room conversations are carried by cable as far as the main terminal ("Bulb" Room) in the basement of the West Wing and could be tapped at any point along the way.

Responsibility for Protection of Telephone Systems

Secret Service has exercised some responsibility for the security of telephone service running through the White House board as a part of its general countermeasures activity. Until 1959, however, the Steering Group

was told that the telephone company kept terminal rooms in the White House locked to Secret Service inspection. Since that time, the company has been slow to share with the Secret Service basic information concerning the system necessary to a thorough assessment of security.

The intermixture of telephone service makes the drawing of lines of responsibility for telephone security between the Secret Service and WHCA a difficult matter, especially if we move to a combined switchboard in the EOB. In view of the fact that a major portion of the telephone security is encompassed in a strong audio countermeasures program, we believe that the Secret Service should assume responsibility for security of all non-crypto-secure telephones. WHCA should continue its responsibilities in the area of crypto-secure systems. However, even this line will tend to blur in the future as more crypto-secure voice service is introduced into White House offices, especially if secure and non-secure service is provided in the same "call director." Thus, the assignment of responsibilities should be reviewed periodically by the proposed White House Security Officer, and others he may designate.

As indicated earlier, we recognize the problems for Secret Service management posed by the addition of these and other technical responsibilities. In the communications area, it would be expected that the Secret Service would call on staff of the DTM and WHCA as needed.

Crypto-Secure Telephones

The only way that telephone calls outside the White House compound can be completely protected is through use of crypto-secure voice systems. Marked improvements in quality are being made, and the new KY-3 telephone is equal in quality to that of regular telephones. These should be installed at vital White House links as soon as feasible, especially in the links to offices and homes of key national security advisers. (KY-3 facilities now exist from Mr. Bundy's office to the Secretary of State and to the ranch.) However, the new secure voice service should not be made available to the President until it has been proven elsewhere and will clearly meet his needs.

Communications at the LBJ Ranch

The major vulnerability of communications at the LBJ ranch is, of course, the mobile radio telephone system, including the "LBJ net." This net can be easily monitored by anyone within a 35-mile radius.

A second vulnerability is the microwave and open wire carrier systems from the ranch to Austin. Both of these can be monitored, although special equipment is required. The microwave system can be monitored with proper receivers from as far as 5 - 10 miles from the microwave towers.

The committee has explored with telephone company staff the possibility of installing a combination of (1) a digital carrier system (such as the T1 carrier currently in use in the Bell system), and (2) crypto-secure facilities to protect the ranch - Austin microwave link. These specially

protected circuits could be used for particularly sensitive conversations, although the long-distance private-line circuits from Austin to Washington remain as vulnerable in the exchanges as they are today (see Appendix __, page __).

Compromising Radiations (TEMPEST)

It was found that WHCA had not had a TEMPEST check at the White House since 1962, although standing procedures called for inspections every year. The preliminary inspection of the WHCA communications area in the East Wing Shelter, initiated as a part of this survey, showed the following:

- Use of high-level teletypewriter cryptographic equipments, which under previous tests have been proved to produce compromising emanations.
- Unfiltered telephones located in close proximity to the crypto teletype complex. The physical separation of equipments was not adequate.
- Inadequate shielding, grounding, and separation of secure and unsecure signal lines.
- Numerous extraneous cables throughout the facility which are potentially hazardous.

These corrections have now been made, and a TEMPEST check has been completed..

Similar conditions were found on review of the cryptographic and communications equipment in the International Situation Room of the

White House. However, the scope (and potential pick-up) of these radiations is considered potentially more dangerous, because the Situation Room is at ground level on West Executive Avenue. TV trucks and other vehicles parked in the area pose a potential threat. One of the "hot" signal cables is located less than three inches from an outside TV antenna, and another runs along an outside wall on the West Executive Avenue side. Also in this area, there is potential inductive pick-up on control lines for the Western Union step clocks. These problems still await correction, after which a TEMPEST check should be made.

The situation in the WHCA communications trailer at the LBJ ranch was basically the same as that at the White House - i.e., the cryptographic equipment was programmed for high-level operation. Readable signals were obtained by Army technicians near the overhead, open wire carrier from the ranch to Austin, many miles from the ranch. It is apparent that from this that the "clear text" radiations were getting into both the open wire carrier and microwave system to Austin. Following conversion to low-level key teletypewriter equipment and other steps to correct installation deficiencies, a final TEMPEST check at the ranch is now under way.

The location of microwave towers in close proximity to the crypto communications at the ranch has the potential of flooding the communications area and providing an escape medium for the reflected energy. This possibility is to be carefully rechecked in the final TEMPEST check.

~~SECRET~~

Recommendations with respect to compromising radiations are contained in Appendix ____, page ____.

White House Office Machines

The survey group attempted to identify automatic office equipment which might radiate recoverable intelligence. On inspection, it was determined that the Xerox machines used for classified information in the White House and the EOB constitute no risk. However, the two Flexowriters, two Royaltypers and four Robotypers used in room 59 of the EOB under the administrative control of the White House do represent a potential hazard and should be used only for unclassified or, at most, confidential information.

~~SECRET~~

i

CONCLUSIONS AND RECOMMENDATIONS

A. Organizational conclusions and recommendations

1. There is no clear responsibility for planning communications in the White House, particularly in technical areas. No one can visualize the whole complex in terms of Presidential and White House staff needs, and take necessary actions. The potential of the Director of Telecommunications Management (DTM) in filling the technical portion of this role has not been adequately recognized and exploited, nor is he presently staffed to perform this function effectively.

We recommend that the Director of Telecommunications Management be given responsibility for technical planning of the telecommunications needs of the President, the White House, and the Executive Office complex, and given adequate staff to perform this function.

2. Although the Secret Service undertook some tasks involving telephone security, its role was not widely recognized. It has only recently been consulted with regard to changes in the system. Without basic records available to the Secret Service, the security program has been hampered.

We recommend that the Secret Service be given responsibility for the security of those communications that are not cryptographically protected, and that an adequate staff be provided for this function, perhaps with a leader on loan from larger agencies.

3. WHCA should be viewed primarily as an operating agency to provide secure communications and all communications while the President is on travel or at emergency relocation sites. Clear guidance to WHCA from the White House is required and is not now being provided.

We recommend that a Presidential Assistant be given responsibility for operational policy guidance to WHCA, and that he use the resources of the DTM for technical advice.

4. The President while in Washington will need to be served

S&T #472

~~SECRET~~

This document consists of 35 pages + 9 charts
No. 4 of 6, Series Draft A

by a combination of WHCA and civilian operated communications, and based on present patterns, primarily the latter. There is a great need to review this relationship to determine optimum organization and balance, particularly as more and better cryptographically secure communications are introduced.

We recommend that the Special Assistant responsibility for policy direction of the communications should initiate a review of the organizational and technical balance of functions between civilian and military communications, keeping in mind the need for privacy and security, as well as efficiency.

B. General technical conclusions and recommendations

1. A normal telephone system which goes outside the White House-EOB complex cannot be made completely secure, even if all recommendations made are carried out.

We recommend that the new high quality secure phone systems be installed and used as much as possible, particularly in circuits to homes of key personnel.

2. Telephone users do not understand the vulnerability of the system to intercept. Clicks on the line which are heard occasionally are normally due to an operator checking the line to see if the call is completed. Clicks can also result from maintenance people checking lines, and very infrequently from natural phenomena. There are no easy ways of determining that a telephone tap exists other than be detailed physical inspection.

We recommend that telephone users be briefed on the vulnerability of the system to intercept.

3. Telephone maintenance and operator personnel have the greatest opportunity to intercept calls, as well as to enable others to intercept them.

We recommend that those telephone personnel assigned permanently to the White House be given a full field investigation by the FBI.

~~SECRET~~

~~SECRET~~

iii

4. The mobile phone networks have no privacy and can be monitored in the Russian Embassy.

We recommend that consideration be given to the use of "Bellboy" service by the key White House staff. Under this system a buzzer rings in the staff man's pocket which tells him to call the White House operator. This call can be made from a pay phone. As an ultimate goal, consideration should be given to installing the KY-8 system when it becomes available.

5. There is insufficient knowledge of the detailed need for secure communications. It is essential that these services be designed so that they are convenient to the user, as well as technically secure.

We recommend that the DTM plan the secure communications system after having made a careful study of the technical and psychological communications needs of the users.

C. Specific technical conclusions for the Washington area

1. The basic telephone system serving the White House is old and fast reaching its capacity. It does not provide an adequate base for future development and was not designed with security in mind.

We recommend that a new system for the White House be developed. This is a particularly good time to consider a new telephone system with desirable security features because of the plans for a new White House switchboard, the renovations in the EOB, and the construction of F.O.B. #7. We believe that the DTM should plan the system with the assistance of the DCA, GSA, and the White House Clerk, under policy guidance from a Presidential Assistant.

2. The present private line service from the White House to the residences is more vulnerable to intercept than normal service. Outside the White House these lines pass through two or three telephone exchanges where they are 'tagged' to ensure special service. In the exchanges they may be monitored by maintenance people even more frequently than other lines in order to ensure quality and reliability. The most vulnerable part of the system, however, is between the last

~~SECRET~~

~~SECRET~~

exchange and the home of the person being called, and both the private line service and the normal service are easiest to intercept over that last link, and in general follow the same path.

We recommend that secure phones be put into these homes when available. We also recommend that a study be made as to the value of direct service to the White House compared with the increased risk of such service. Finally, we recommend that the Secret Service check the private lines to key residences and offices through the exchanges and from the last exchange to the home on a random basis in order to identify and correct obviously insecure conditions.

3. The present White House/EOB system is not designed for security and privacy. There are too many switchboards, and there appears to be more manual operation than is needed by the President and top staff, thus increasing the chance for operator intercept. The internal system is not sufficiently segregated from the outside system, and there is insufficient protection of terminals and frame rooms. NSC personnel must use the EOB lines through the Lafayette Exchange when calling Mr. Bundy's office in the White House. There is an extraordinary amount of extraneous and unused wire and equipment. The Speakerphone systems present additional eavesdropping hazards.

We recommend that, consistent with the best possible service, planning for the White House/EOB complex take some account of privacy and security matters. During the design recommended above the following features should be considered:

- a. A self-contained system serving the White House/EOB complex physically secured.
- b. A combination of manual operation and a flexible dial system so that more calls can be made conveniently without going through an operator.
- c. An automatic disconnect capability so that when the inside telephone is hung up, the line into the White House does not remain open to outsiders.
- d. Some form of operator disconnect on calls that have been

~~SECRET~~

~~SECRET~~

v

established so that the operator cannot re-enter the circuit except on recall by the parties.

e. As an interim measure, NSC staff should operate off the White House automatic board.

f. Unused wire and equipment should be removed as far as practicable.

g. Terminal boards should be locked.

h. Frame rooms should be secured.

i. The Speakerphone service should be examined to see if satisfactory service can be provided with greater assurance of privacy.

4. Outside the White House there is insufficient inspection of cables, manholes, and exchange equipment. The most valuable (and difficult) area for a telephone tap is the main cable between the White House and the central exchange.

We recommend that the Secret Service inspect the cables, manholes, and exchanges at random intervals. We also recommend that a study be made of the possibility of using digital carrier encrypted for privacy between the White House and the first exchange to reduce the possibility of intercept along this route.

D. Special technical conclusions and recommendations about the service in Texas

1. The mobile service is highly vulnerable to intercept.

We recommend that the possibility of using the KY-8 service when it becomes available be considered.

2. The microwave link and the open wire carrier between the LBJ ranch and Austin are vulnerable to intercept.

We recommend that the possibility of using encrypted digital carrier over these links be considered.

~~SECRET~~

~~SECRET~~

vi

3. Some terminal boxes are not protected against access.

We recommend that terminal boxes on the ranch be
secured.

~~SECRET~~

~~SECRET~~

(r a f t #3:DZROBINSON
7 April 1965

TELEPHONE SECURITY AND PRIVACY

I. GOALS

This section will:

- A. Briefly describe the telephone service available to the President and his top staff.
- B. Describe the various threats to security and privacy of telephone conversations.
- C. Make recommendations which will improve the probability that there will be no intercept of telephone conversations.

II. GENERAL APPROACH

The communications sub-panel approached the problem of examining the security of telephone service of the President and top staff in the following ways:

A. Telephone service in the White House-EOB area

1. The panel surveyed the telephone service in the West Wing, the Mansion, General Clifton's area in the East Wing, and the National Security Council area in the Executive Office Building. In particular, the main terminal rooms in the White House and EOB were examined, as was the local cabling and wiring in selected areas of the West Wing and the Northwest corner of EOB.

2. Fourteen of the special circuits which bypass the switchboards were traced.

3. Discussion of organization and practices were held with the Secret Service, the White House Communications Agency, the Defense Communications Agency, the White House Clerk, and those representatives of the C & P Telephone Company who had responsibility for the White House service.

~~SECRET~~

~~SECRET~~

-2-

B. Telephone service in the Washington area

1. The cable diagrams between the White House and the major exchanges were obtained from the C & P, and the routes were checked.
2. Major switching areas were examined.
3. The service to the homes of twelve people likely to be involved in matters where privacy or security were important -- the Vice President, Secretary Rusk, Secretary McNamara, Under Secretary Ball, Under Secretary Vance, Mr. McCone, Mr. Bundy, Mr. Busby, Mr. Moyers, Mr. Reedy, Mr. Valenti, Mr. Watson -- was examined.
4. The characteristics of the mobile system were examined.

C. Telephone service outside the Washington area

1. The type of service available to the President during travel was surveyed with the help of the White House Communications Agency.
2. The service to the LBJ ranch was examined and discussed with representatives of Southwestern Bell, and the WHCA.
3. The ninth floor of the Federal Office Building in Austin was surveyed.

D. General briefings

The general problems of telephone privacy and security were discussed with representatives of the FBI, the CIA, NSA, and the AT&T.

III. ORGANIZATION OF TELECOMMUNICATIONS IN THE WHITE HOUSE

Two major groups are responsible for Presidential telecommunications. The White House Administrative switchboard (the "Administrative Board") takes care of about 90% of the day-to-day communications of the President and top staff in the White House itself; the White House Communications Agency (WHCA) is responsible for some of the day-to-day traffic, White House Police communications, all the cryptographically secure communications,

~~SECRET~~

~~SECRET~~

-3-

all the out-of-town communications, all mobile communications, and all communications at emergency locations.

A. The White House Administrative Board

This switchboard is located in the Executive Office Building, and has grown from a two-position switchboard in 1932 to a ten-position switchboard today. It is under the general supervision of Mr. Hopkins, the White House Clerk.

Policy direction for this switchboard has come from a Special Assistant to the President in recent years. Mr. Hopkins has looked for guidance from Matthew Connolly, General Carroll, General Goodpaster, Kenneth O'Donnell, Walter Jenkins, and now Bill Moyers.

Technical assistance in the design of the telephone system has come from the C & P Telephone Company.

B. The White House Communications Agency

The WHCA performs a number of functions as described above.

In 1954 the Agency was called the White House Army Signal Agency and was placed under the Office of the Chief Signal Officer. There was no official policy guidance, but the staff of the agency was responsive to the desires of the military aides, the presidential staff, and the President. In general, WHASA tried to anticipate Presidential needs.

Since WHASA was an operating agency, it obtained technical assistance from the military services (particularly the Signal Corps), from the C & P, and from AT&T.

On 31 August 1962, after a letter from the President to the Secretary of Defense, the Agency was established as the White House Communications Agency, and P. Kenneth O'Donnell was formally named as communications officer responsible for policy direction. It was anticipated that broad requirements would be established in consultation with the Military Aides, and the Special Assistants for National Security Affairs and Science and Technology. Actually, this latter group was never formally convened, but there were discussions between them on specific issues affecting the service.

~~SECRET~~

~~SECRET~~

-4-

Programming, budgeting, and funding for the WHCA are the responsibility of the Defense Communications Agency.

C. The Special Assistant to the President for Telecommunications

The appointment of James O'Connell as Special Assistant to the President for Telecommunications was not made until 1964. Mr. O'Connell has responsibilities under an August 21, 1963, Memorandum from the President to "Identify communications requirements unique to the needs of the Presidency."

The Special Assistant has carried out these duties by submitting requirements to the DCA for implementation of the command and control needs of the President, but has not been involved in the problems of day-to-day operation of White House communications.

D. Responsibility for security and privacy of Presidential Communications

The White House Communications Agency is responsible for the security and privacy of the crypto-secured Presidential communications. The general reliance for telephone security of the non-secure communications of the President seems to lie with the Secret Service and White House Police inside the White House, and with the C & P Telephone Company outside the White House. There appears to be no formal designation of this responsibility, however.

IV. THREATS TO TELEPHONE SECURITY AND PRIVACY

Before describing the Presidential service in some detail, the general problems affecting various types of threat to telephone security and privacy will be described.

A. Threat to non-secure voice systems

Although all systems which do not use cryptographic security are vulnerable to intercept, the ease of intercept depends on the system which is used, since some systems are more vulnerable than others.

The vulnerability of a particular call is limited by the number of links and by the strength of the links. It does little good to secure a relatively strong part of the circuit, if relatively weak links still exist.

~~SECRET~~

~~SECRET~~

-5-

The vulnerability of the telephone system to intercept depends both on the technical configuration and the ease of accessibility to an agent. The system is particularly vulnerable to an agent who has access to the system normally. The essential elements to successful intercept are:

-- a tap, which may be either a physical or an inductive connection.

-- a listening post, which can be remote from the tap by using telephone or radio circuits to relay the intercepted conversation.

-- equipment necessary to convert the line signals to audible. This equipment is complex when microwave carrier is used.

Many times vulnerability of a system can be reduced by the sheer bulk of traffic and the diversity of paths that exist in the American telephone network. Particular attention should therefore be paid to the parts of the system where there is little or no choice of paths (e. g., homes of key officials).

The following are the types of communications used, together with the description of the vulnerability.

1. Mobile phones: All mobile phone systems which are not cryptographically secure are easily monitored by anyone in a large area. This applies to automobile telephones, as well as helicopter and aircraft phones.

2. Microwave circuits: A great deal of long distance transmission is over microwave relay. Although the demodulating equipment is expensive, a determined person anywhere in the area of a microwave system can record the conversations made.

3. Internally switched systems: An internally switched system (such as the White House administrative board) is vulnerable to penetration only inside the area where it exists when used for local calls. It is possible for an operator on a manual switchboard to monitor the call, and to that extent a manual board is more vulnerable than an automatic board.

~~SECRET~~

~~SECRET~~

-6-

4. Externally switched systems: Externally switched systems, such as would be used from EOB to the White House, are potentially vulnerable to penetration not only in the compound itself, but also in the lines between the compound and the exchange which does the switching. In addition, in the exchange the lines are available to test operators and maintenance men.

B. Secure telephone and teletype

1. Extensions. The major threat to a cryptographically secure telephone system lies in the part of the system between the crypto equipment and the subscriber. Obviously, if anyone listens to an extension of a secure phone, he can hear the conversation.

2. Pick-up or tap along the cable between the subscriber set and the crypto equipment. Regular teletype and telephone equipment will radiate signals in the air or along the wire line. Obviously this radiation can be picked up if there is the right equipment nearby. Telephone conversation might be picked up by direct tap of the phone line, or by induction from a nearby line. For this reason NSA standards do not permit secure telephones to be established as special keys on call directors at the present time, since the number and crowding of wires inside the telephone set may lead to potential interception through pickup on the non-secure lines.

3. TEMPEST. With modern techniques of detection it is possible under various circumstances for the "clear" messages to be recovered. These problems arise in the design of the communications system and are normally considered under the code word TEMPEST. The problems arise particularly on secure teletype equipment which had been developed some time ago and are now a major item in the inventory. In general, some modifications usually must be made and certain design standards must be met in order to avoid these compromising signals.

Despite these problems in design, cryptographically secure systems are far less susceptible to breach of security and privacy than even the most imaginatively designed normal system.

C. General principles of technical privacy enhancement

A few general principles of enhancement of privacy can be stated as a result of the above analysis. Since these principles were followed in making the recommendations, they are stated explicitly here.

~~SECRET~~

~~SECRET~~

-7-

1. Use as much crypto-security as feasible and convenient.

The new systems which are becoming available give as good quality service as normal phone and are reasonably inexpensive for short distance communication.

2. Do not use unsecured mobile systems. The number of receivers now available is so great that there must be a large number of people listening on Presidential calls today. The Panel has heard of breaches of privacy on the present mobile system.

3. Be as self-contained as possible. Terminals and switching equipment should be under the control of the user and located in a secure area.

4. Be as automatic as possible. Automatic systems are harder to break into than manual systems. Of course, service needs may still require manual operation of portions of the system.

5. Keep the service as simple as possible. Complex organization, large numbers of subscribers, large numbers of boards and terminals, and extra types of service, make it difficult to ensure privacy.

6. Remove unused wires, terminals, and equipment. Wires of unknown use are potential hazards and should be removed.

7. Keep up to date records.

V. DESCRIPTION OF WHITE HOUSE TELEPHONE SERVICE WITH EMPHASIS ON VULNERABILITY TO INTERCEPT

A. Service in Washington, D. C.

1. Mobile phone systems

A mobile phone system is used to reach people in White House cars. This system operates on bands between 200 and 400 Mc, and is known to have been intercepted by private citizens. A radio link also operates between the White House and the helicopter while it is being used.

2. Non-secure telephone service in the White House and EOB

a. Switchboards

Of three manual switchboards in use in the compound, the

~~SECRET~~

~~SECRET~~

-8-

White House Administrative Board is primarily for administrative needs of the White House and staff. This ten-position board, located in Room 405 of EOB, intercepts all incoming traffic on the official telephone number 456-1414, and provides normal telephone service. Also connected to this board is private service to the offices and homes of many of the President's staff, i. e., cabinet members, principal assistants, his secretary, etc. The operators have available to them FTS trunks (Federal Telephone Service), IDS (Interdepartmental Service or Government Code) trunks, trunks to the Signal Board, and trunks to the Lafayette exchange.

It is not possible to ring directly to the President on this system. All incoming calls must go through his secretary. It is possible, however, for the President to dial out from his office and not go through the operator. The telephone operators are required to keep track (if possible) of who is in what office, who is at home, where an official may be, if he is out of town, keep a log on what "crank" calls were received, and a log on troubles reported. All calls to and from the President are handled by positions 1 and 2, and usually by the Chief Operator. These calls can be monitored by the operator with or without the knowledge of the parties involved.

The White House Communications Agency has a Signal Board and a Police Board located in the shelter area of the East Wing. The Signal Board provides service similar to the Administrative Board, both internally and to the homes of many of the more important members of Government. (In some cases there is a duplicate of the administrative service to VIP homes.) This board has two-way trunk lines to the Administrative Board, Autovon, Inter Departmental Service (to all other Government organizations) and commercial lines. While there is no direct service from the President's office out through this Board, the operator has a line direct to the President (#192), that rings in his lounge and is not available to anyone, including Miss Roberts. All manual calls can be monitored by the operators with or without the knowledge of the President.

The Police Board, a multiple of the Signal Board, is primarily for the use of the Secret Service and White House police guards. This board connects to all guard posts, control points, police office in East Wing and the security office in EOB for internal controls. This Board has the same capacity of the Signal Board, but in normal operations all except police lines are blocked by small removable plugs. By removing these plugs, an operator could listen to conversations that may be in progress on the Signal Board by plugging in on the line.

~~SECRET~~

b. Switching equipment and cables in EOB

The automatic switching equipment (300 lines), connected to the Administrative Board is located in EOB Room 578. Thus, all terminations on the Board appear in this room. A small PAX (Private Automatic Exchange ST 3-9377), used primarily by the White House Communications Agency as a two-digit dial intercom (with most of the lines being located at 517 - 26th Street, N. W.) is also located here. This PAX also has the capacity of making calls to, but not the capacity of receiving calls from, the commercial exchanges. These two pieces of automatic switching equipment are only about 20% of the total equipment located in this room, but are all that is working. In addition, about 20% of the local house distribution cables in Room 578 have been cut at the frame. Of the remaining cables, about 15% are in use. It was not possible to determine the number of wires that were connected to either unused pairs or dead equipments in the time allotted.

In Room 045 of EOB, government cables were easily identified. House cables for the EOB were readily identified but a little more difficult to trace. The "Wire Closet" was in poor condition with the installation of cables coming in two different ways: (1) through a hole in the wall with large cables going toward a manhole outside the building, and (2) over the door to the hallway. The cables going out the door became the main distribution system. (As the door opened and closed it was wearing the insulation from the cables with bare wire showing through. The door had been cut away at the top to make room for the cables.) These local house cables were strung along the ceiling of the hall among the collection of pipes. Along the wall, near the ceiling, there had been some bricks removed from the original construction revealing a heating flue. These heating flues became the risers conduit for the cable distribution system. Since the original cable riser installation, miscellaneous wires and cables have been added. These are very difficult to trace because they all have been painted the same color, besides being buried among the pipes. The risers themselves are not too difficult to find; however, local house pairs on the main frame that had cross connections did not necessarily have the same connections in the house box in the floors above.

In the general area of Room 045, there were cables and terminal boxes that are not in use, some of which do not belong to the telephone company.

~~SECRET~~

~~SECRET~~

-10-

c. Condition of switching equipment and cables in the White House

The Bulb Room is located in the West Wing basement. The main cables (63A and GOV 6) entering here were easily identified. With no line record cards available to the installer in the Bulb Room, it was impossible to determine what cable pairs were cross-connected, but not in use. (63A had about 80% of its pairs in use and GOV 6 had about 55% of its pairs in use.) The East Wing cable which joins the Bulb Room to the signal main frame was completely filled except for 30 to 40 pairs which are bad. The local distribution cables in the West Wing are limited in number and being replaced as rapidly as possible. In this area, new Alpeth cables (100% shielding) are being run directly from the instrument to the Bulb Room through conduit (with a quantity of cable coiled up for extension later to a new equipment room) with no splices or terminals in between. Eventually, all telephones in the West Wing will be installed in this manner. At the present time, the President's phones are installed directly to a separate small wire closet in the basement, but are not in shielded cable. The secure extension cables are either in an alarmed area or in conduit.

The main terminal for local distribution on the second floor of the White House is located in the old switchboard room. This terminal and the local panel boxes on all floors are not locked, but are in a semi-controlled area.

In the Program Control Room, located in the basement of the mansion, there is a number of TV circuits and amplifiers. Also installed here are some miscellaneous telephone equipments and cables that are for local distribution and access to the main telephone rooms in both East and West Wings.

All the above mentioned main terminal areas are alarmed and controlled by the Secret Service alarm panel in Room 097, EOB. While these are relatively secure, the local house terminals in all areas are only partially controlled, since the terminals are in the White House and EOB controlled areas. They are not locked and anyone that can gain access to the area would have access to the telephone terminals.

d. Telephone extensions and accessibility of terminals in the White House

A survey of the telephone service being provided throughout

~~SECRET~~

~~SECRET~~

selected areas was completed. All of the West Wing was done with the exception of the Bundy offices which were occupied each time the inspection team tried to enter the area.

The President has only one non-secured telephone number (#192 on the Signal Board) that does not have an extension outside his office in the White House. Connected to each call director (of which there are five) is a speaker phone which is usually turned on full volume. Thus, all conversation in the offices can be heard over the speaker phones. All incoming calls are received first by his secretary. The President also has a number of private direct lines to his principal assistants. However, his direct lines to Moyers and Valenti appear on each other's call director and cannot be strictly classified as "private", since someone in one office could hear a conversation in the other office.

Most of the rest of the West Wing telephone service has a similar pattern, with some private lines, and many manual lines from the White House Board or Signal Board, or both. With few exceptions these lines can be monitored by people in secretaries' or assistants' offices, or by telephone operators, with very little difficulty.

The Cabinet Room had an extension of the White House Board mounted on the conference table with an extension on Miss Roberts' desk.

The Conference Room telephone on the second floor has an extension of all the numbers of Mr. Feldman and Mr. O'Brien.

The Lobby and Press Room area had a great number of automatic tie lines and private circuits to outside exchange numbers, mostly going directly to the home office of press and radio members. Located in the Press Room is a local house terminal box providing service to the area through four smaller local cables and terminals.

The "Dog House" had a local house terminal box in the room and many special circuits for radio broadcasting. It was impossible to trace all the circuits in here without disassembling the equipment in the room.

WHCA Recording Studio has 75 pairs directly from the Bulb Room terminated in the rear room next to the recording equipment.

~~SECRET~~

~~SECRET~~

-12-

It would be a simple matter to connect any line in the Bulb Room to the cables to the recording studio and attach a recorder with or without permission.

The Mansion itself had few telephones in comparison with the other areas. All instruments with one exception went directly to one of the manual boards or the dial equipment located in the EOB.

e. Special services

There are a great number of lines entering the White House-EOB compound that bypass the operator. Many of these numbers are special circuits for radio, TV, and press coverage of the White House. All of the three digit numbers on the White House Board may be dialed directly from any Government code bypassing the operator. However, the operator may still monitor this call, if desired, by plugging into the right jack on her board. All of the five digit numbers in EOB (Code 128) enter the compound directly from the Lafayette exchange, bypassing any operator. The operators in the EOB and the White House have no way of monitoring these circuits.

Fifteen special circuits that enter the compound were selected at random and traced as much as possible. All the circuits were identified on the feeder cable with relative ease, and traced to the distribution cables. At the distant terminal all but parts of two circuits could be traced to their ends. One part of circuit 10PL 2486 could not be traced in the East Wing and the telephone man did not know where it went. On part of circuit 12PL 2744 was tied to a West Wing terminal that had a wire on it that could not be traced. It went into a plastered wall.

~~SECRET~~

~~SECRET~~

-13-

3. Secure Telecommunications Systems Supporting The President At The White House

There are two basic secure telecommunications services currently provided at the White House to support the President and his immediate Staff. These are identified as secure teletypewriter and secure voice-service.

a. Secure Teletypewriter Service

The White House Communication Center located on the lower level in the East Wing of the White House provides for normal transmission and receipt of messages in either a secure or non-secure mode to locations indicated on Chart I. The Center receives and delivers messages to the White House Situation Room via a pneumatic tube which inter-connects the two locations. In addition, teleconferencing can be established from either the Situation Room or the Communications Center to locations world-wide which have comparable capabilities.

b. Secure Voice Service

Secure voice service provided at the White House permits access to a number of different secure voice networks and interconnection to various subscribers. This service is identified as:

(1) Secure Voice Low Quality Service. From the White House Situation Room, connections can be made through the White House Signal Switchboard to a number of locations either directly or through other intermediate switchboards. The various locations which can be contacted are identified on Chart 2. The KY-9 speech security device is the instrument which provides the communication security between the terminal points. It is a half duplex system (it works in only one direction at a time) and requires the user to depress the "push-to-talk" button on the telephone hand set when speaking.

(2) Secure Voice-White House to Ranch - high quality service. A high quality secure voice link has been established between the White House Situation Room and the Communications Complex at the LBJ Ranch in Texas as depicted on Chart 3. The KY-3 speech security device provides the communications security and the telephone instrument is used in the same manner as a normal telephone.

~~SECRET~~

(3) High Quality Secure Voice (in town) Service.

A high quality secure voice service is provided from specific locations within the White House to certain other locations primarily within the Washington area. Special telephone instruments installed within the White House are connected to the White House Secure Voice Switchboard through which the various other points may be reached as indicated on Chart 4. The KY-1 speech security device provides the communications security and the telephone instrument is used in the same manner as a normal telephone.

(4) High Quality Secure Voice (out-of-town) Service. This is basically the same service as the "in-town" but permits the users in the White House identified in Chart 4 to reach locations and users outside the Washington area as identified in Chart 5. The KY-1 speech Security devices currently used in both the "in-town" and "out-of-town" nets will be replaced by the later KY-3 device as soon as sufficient numbers of equipments are obtained to permit complete replacement at all locations simultaneously.

(5) Twilight Network High Quality Secure Service. A special secure voice service is provided at the White House Situation Room to connect with No. 10 Downing Street in London. As indicated on Chart 6, this service uses a voice security device provided by the British and requires pre-arrangement before it can be used. On a "crash" basis, the circuitry can be established within 30 minutes. However, normal time for establishing the service requires approximately two and one-half hours.

In addition to the secure telecommunications services currently being provided, testing is under way on a system to permit secure voice and secure teletypewriter services between the White House and the Presidential Aircraft. This proposed service would permit the President to be in contact with the White House during flight and ultimately permit interconnection through the White House communications facilities to world-wide locations.

~~SECRET~~

4. Exchanges

The telephone service from the Administrative Board and Signal Board leaves the White House compound in two cables, one to "Mid Town" and one to "Downtown" exchanges. Each of these exchanges was guarded and visitors were required to sign a register and be escorted at all times. The cables were identified and each circuit of importance was protected by a cap over the terminals. This cap meant that the employee was instructed never to enter the circuit unless directed to do so by a supervisor. Also at the downtown office, the White House cable pairs had a sign in place reminding the maintenance personnel to use no audible tones in trouble shooting on these circuits.

In a visit to the Dupont and Woodley exchanges, it was determined that the special circuits were handled in the same manner as downtown. The security of the buildings was less stringent, but adequate since they are manned 24 hours a day.

The tapping of a cable between the exchanges or the main distribution cables from the last exchange to a private home would be a great undertaking and it is felt that the small amount of intelligence obtainable would not justify the expense or risks involved, particularly since the final cable near the home is so easy to tap.

In each exchange the maintenance personnel has the capacity of monitoring the lines without the knowledge of the parties involved. The test desk operator in the exchange that assigns the central office equipments to a line can dial in on a circuit and listens without being discovered, even if the circuit is busy. The local telephone operator also has the ability to dial undetected into a busy circuit by using her verification jack. Furthermore, the special protective features (cap over terminals, sign stating that no audible tone should be used on the circuits) call attention to the Presidential circuits in the frame room.

~~SECRET~~

-16-

5. Staff service outside White House

This section covers the security of off-premise extensions of the Administrative Board and the Signal Board for the following persons:

	<u>Admin. Board</u>	<u>Signal Board</u>
Vice President Humphrey		x
Secretary Rusk		x
Secretary McNamara	x	x
Mr. McCone		x
Under Secretary Ball	x	
Deputy Secretary Vance	x	x
Mr. Bundy	x	
Mr. Busby	x	
Mr. Moyers		x
Mr. Reedy		x
Mr. Valenti	x	x
Mr. Watson	x	x

The service was traced from the wire center (exchange) serving the residence to the residence itself.

a. General

In general, service leaves the last wire center from a cable vault and proceeds underground in large cables containing from 900 to 2400 pairs. The cables run through manholes where they either go straight through or are spliced. Periodically, cables branch into smaller cables taking different routes to provide service to various geographical areas. Cables leave the ground and travel on overhead wire, usually near the residence, but in more remote areas for some distance via aerial cable, before terminating on a pole from which service is provided to the residence. Generally cables are reduced to approximately 25 pairs before ending on lugs in terminal boxes from which service to the house is provided. In several cases as described in the detailed description, service is provided by means of spliced cables directly to the residence to eliminate the appearance of pairs on the poles. In all cases detailed examination of the wires permits visual tracing from the residence to the terminal box or splice which provides residential service.

~~SECRET~~

~~SECRET~~

-17-

Vulnerability to unauthorized access is greatest in the aerial runs near the residences, particularly in the terminal boxes where pairs appear on terminal lugs.

As a general rule, the allocated circuits from the White House boards are provided from the same cable terminal strip as is used for regular commercial service to the residence.

In the physical survey of the facilities by members of the Survey Group, it was apparent that no particular difficulty is encountered in detailed scrutiny of the poles, wires, terminal boxes, etc. which provide service. On two occasions when people were encountered, the statement, "We're with the telephone company" satisfied their curiosity and stopped any further questioning. One party in fact assisted in the determination of a pole number which was not visible from the point of team observation. No identification was requested nor was the fact that they were telephone company personnel challenged. On the basis of this experience, it is believed that anyone wishing to do so could take almost any action with respect to tampering with the lines in question with very remote possibility of detection or challenge.

b. Specific description

The descriptions that follow generally start with the residence and work toward the serving wire center.

The Vice President -- Service to the residence is from a splice on a pole across the street from his house to an underground run beneath the street into his basement. His service, however, is aerial from the residence to a manhole at Dunlap Street and Connecticut Avenue several miles distant. Much of this area is slightly developed and in several areas is screened from sight from all houses.

The neighborhood in which the Vice President resides is normal residential.

Secretary Rusk -- The pole providing service to the residence is in the rear in a wooded area bounded by Quebec Street, Glenbrook Road, 49th Street, Rockwood Parkway and Fordham Road. There are five appearances of Branch 512 of the Signal Board in this area, three on poles and two in terminal boxes in manholes. There are

~~SECRET~~

~~SECRET~~

-18-

two appearances of Branch 2321 of the Administrative Board on poles in this area and one more in the area bounded by University Lane, Quebec Street and Woodway Lane. Access to the poles and manholes appears relatively easy, particularly in the wooded areas behind the houses. Circuit pairs can be visually traced from the residence to the pole line and thence to the various terminal boxes in which they appear.

The neighborhood is medium density residential, lots are large with much open space, rather heavily wooded, to the rear where pole lines are located.

Secretary McNamara -- Service is provided by means of underground cable from the basement of the residence to the rear wall of the back yard, thence above ground in lead conduits towards 24th Street. At the corner of 24th Street and California Street a cable is affixed to the side wall of the Finnish Embassy where it proceeds to the corner before disappearing underground to a manhole in the intersection of 24th and California Streets. An employee of the Finnish Embassy (a Finn) stated facetiously (it is believed), as we reviewed the cable run, "Mr. McNamara has his lines in this cable; we listen to him all the time."

In the review of this facility we had reason to enter the McNamara residence to examine the terminal strip in the basement. We identified ourselves to the maid as "telephone company men" and she admitted us without question. We proceeded to the basement, unescorted, and spent some five minutes examining the terminal arrangement. At no time were we asked to show identification.

The neighborhood in which Secretary McNamara resides is high density residential. The service is shown on chart 8.

Mr. McCone -- The line record cards on file in the Dupont Wire Center show that the pairs serving Mr. McCone's residence terminate in the basement of the main building at 3100 Whitehaven Street which is identified as the Center for Hellenic Studies, a complex of buildings inhabited by students of many foreign lands, and in a terminal box on a pole across the street from the residence. On the first visit to the area by the Survey Group, one of the C&P representatives confirmed that this had been the case but that it no longer was true. A recheck resulted in the

~~SECRET~~

~~SECRET~~

-19-

telephone company producing a later engineering drawing dated December 16, 1964, and of satisfactory verification by the Survey Group that the appearances indicated in the line record cards were in fact erroneous. It would appear that the service was changed not long before the date of the new engineering drawings.

It was determined that Mr. McCone's service was spliced from a short aerial run approximately one-half city block directly into his basement.

The neighborhood in which Mr. McCone resides is high density residential except for the Center for Hellenic Studies and the Danish Embassy which is adjacent thereto.

Under Secretary Ball -- Access to the pole line from which his service is provided is through the yards of the residences to the rear. One of the neighbors came out to determine the reason for her dog barking as we proceeded towards the rear of her house down the driveway. Again, when told that we were from the telephone company she asked for no identification and returned to the house. We proceeded to the pole line and spent some fifteen minutes developing the necessary information without further challenge. Under Secretary Ball's service appears in terminal boxes on two poles in the block square area on which his house is located. These are accessible through the yards of surrounding houses.

The neighborhood in which Under Secretary Ball resides is high density residential and most yards are fenced.

Under Secretary Vance -- The terminal box on which his line appears is on the cable and is accessible only by climbing a pole which is directly across from the house. Anyone who made the effort probably could tap the line at that point.

The neighborhood in which Under Secretary Vance resides is highly developed and the pole which serves his residence is located on Foxhall Road in sight of six or eight houses.

Mr. Bundy -- The pole from which his house is served is visible from several houses. However, his line runs in an aerial cable several blocks to Loughboro Road before going underground into a manhole. This aerial run can be visibly traced and access to his line through the terminal box on the pole at Maud and Loughboro Road does not appear difficult.

~~SECRET~~

~~SECRET~~

-20-

The neighborhood in which Mr. Bundy resides is normal residential. His service is shown on chart 9.

Mr. Busby -- The service to this residence travels on overhead wire through a wooded area for several blocks from Massachusetts Avenue and DuVal Drive. A terminal box on the pole at that point is partially concealed from most residences and appears to be readily accessible to anyone making an effort. The neighborhood in which Mr. Busby resides is lightly populated with residential development, with houses about 100 feet apart. The pole which serves the residence is located in the rear yard between Newport Street on which Mr. Busby resides and Cammack Drive to the rear. Access to this pole is only through the yards of the residences and lots are substantially free of heavy foliage. It would probably be difficult to gain access to the line at this point by other than telephone company personnel although it is problematical whether identification would be requested.

Mr. Moyers -- The pole from which service is provided is located across the street from the residence. The line also appears in a BD box on a pole at Sherwood Hall Road and Midday Lane approximately three blocks from the residence. This is a large terminal box about four feet high by 18 inches wide and is mounted about 10 feet above the street. This box terminates the entire cable serving the development and is provided with steps and with a seat to facilitate working on the line terminals. The pole is located approximately 50 feet from a house on a corner but no curiosity was exhibited by any person during the five minutes that the pole was scrutinized and notes were taken. Service from the BD box is by aerial cable back to Boswell Street and Schellborn Road, a distance of several miles. This cable travels through considerable substandard housing areas along Sherwood Hall Road and US 1 before going underground at the manhole.

The neighborhood in which Mr. Moyers resides is a new development about two miles from US 1 near Hybla Valley. The service is shown on chart 10.

Mr. Reedy -- The pole which serves Mr. Reedy's residence is in the back yard of the house next door but the line also appears on another pole over a block away. It was in the checking of this pole that a neighbor asked if she could be of help. When told that

~~SECRET~~

~~SECRET~~

-21-

we were from the telephone company she left her porch and came out to help us read the pole number. No identification was asked for. When the pole was located it was found to have a number of wires hanging loose and unconnected from the 25 pair terminal box which was mounted on the cable. It was not determined what these wires were for.

The neighborhood in which Mr. Reedy resides is residential on large lots, most of which are in back of the house. Back yards are heavily planted and visibility is restricted even in winter. In summer, foliage would further reduce visibility.

Mr. Valenti -- The poles on which the wires to his house appear are all within sight of several houses. Again, accessibility by anyone making the effort would not be difficult by climbing a pole and tapping the terminal box which serves the house.

The neighborhood in which Mr. Valenti resides is normal residential.

Mr. Watson -- His lines appear at three locations each but do not duplicate at one resulting in four locations total. The pole serving his house is across the street and is visible from several houses. Another pole at the top of the road also is visible from several houses. These lines appear, however, also in a terminal box on a pole across the George Washington Memorial Parkway out of sight of all houses. They also appear in a terminal box on another pole 1/2 mile away between 4429 and 4433 Chain Bridge Road. This pole is visible only from the two nearby houses. Accessibility to those lines would appear relatively simple.

The neighborhood in which Mr. Watson resides is normal residential and is sparsely populated.

~~SECRET~~

~~SECRET~~

-22-

6. Assessment of the threat to telephone privacy in Washington

The threat to telephone privacy may be graded as follows:

Group A. The casual or curious individuals who will eavesdrop if opportunity presents itself, but without any other motive than curiosity. This group invades privacy but presents little danger to security except insofar as it may unintentionally repeat information under circumstances which allow it to reach others who make use of it.

Group B. The semi-professional who makes use of information for personal, monetary, or political gain, but who is limited by funds and technical capability.

Group C. The professional backed by virtually unlimited funds and technical talent of high caliber. He may be an intelligence agent or an individual, such as a telephone employee, who is more or less under the control of an agent.

The vulnerability of the presently installed system can be assessed as follows:

a. Radio links, vehicular and aircraft radios vulnerable to groups B+C. It can be assumed that all radio links in the Washington area that carry intelligence of value are monitored at the various Embassies, official residences, and other locations where foreign nationals can operate freely.

b. The telephone system within the EOB/White House compound. The various extensions, speaker phones, and switchboards are vulnerable to groups A + B. The complex can also be penetrated by Group C - the EOB terminals which serve the White House Administrative Board being particularly vulnerable. The EOB complex is not carefully controlled for access, and the precautions in use today were put into effect only a few years ago. It is, therefore, possible that equipment installed several years ago is still operative. The large amount of unused equipment and wire which is no longer in service both in the White House and EOB make inspection extremely difficult and thus the task of an agent simpler.

~~SECRET~~

~~SECRET~~

~~SECRET~~

-23-

c. The outside cable plant (between White House-EOB and the various control offices). Vulnerable to Group C. Although the cable is pressurized and underground, the intelligence value of a tap would make such an effort worth a great deal of time and money. If unobserved access can be obtained (in a manhole), the cable can be tapped without disturbing the user. Such a tap, when once placed, can operate for an extensive period unless compromised by carelessness or physical inspection.

d. Central Offices. The terminal frames and test facilities are vulnerable to Groups A, B, and C, insofar as access to the sensitive areas is not controlled.

e. Cables between central offices. While probably more vulnerable than the White House/EOB-to-central office cables, these present a questionable intelligence target because the particular lines which may be used for a sensitive conversation may be hard to locate.

f. Circuits from central offices to subscriber homes. Vulnerable to Groups B+C. Many of the existing installations provide terminals in readily accessible locations where an agent could operate undetected or posing as a telephone company employee.

g. Inductive pick-up. The large number of circuits, particularly those which are dedicated or private lines which enter the White House/EOB area when taken together with the "unused" wire, which has not been removed, provide a potential means of access to the telephone system by an agent without his ever having entered the complex personally. If an agent can obtain access to one of these circuits outside the complex, it is possible that they will carry (by inductive pick-up) conversations carried on over pairs of wire which pass in close proximity, e. g., are in the same cable.

B. Telephone service available to the President while travelling

1. Mobile systems

While travelling in Presidential aircraft, radio telephones are used. These conversations are monitored for safety purposes by an Air Force contractor, and of course are available for monitoring by anyone with a sufficiently sensitive receiver.

~~SECRET~~

Mobile phone systems are also available to the President if he were to go on a ship.

2. Portable switchboard

When a Presidential party is staying overnight in a city, the WHCA will take over part of a hotel switchboard for the use of the President and his staff. If there is no switchboard available, WHCA will set up a portable switchboard for this purpose. The use of this board eliminates monitoring by hotel staff and gives better service.

C. Telephone service in Texas

1. Description of the service

The service is installed and maintained by the Southwest Bell. The main switchboard (manual), operated by WHCA, is located in a trailer on the ranch property. A buried cable runs from the central office at Fredericksburg to the ranch - thence to the Johnson City central office - thence to the Moursund Ranch. Branch cables go to: (a) Lewis Ranch and Hartmon Hill Radio Station and (b) Sharnhorst Ranch, West Ranch Radio, Nicholson Ranch, Valenti and Haywood Ranch. (See plan and cable schematic for details.)

Trunk service is by (a) three hop microwave to Austin, (b) cable to Johnson City and thence by open wire courier to Austin, (c) cable to Fredericksburg. Various Bell System circuits are utilized from Austin and Fredericksburg onward.

The ninth floor offices in the FOB may be served by either the FOB switchboard or when desired by the WHCA operated board at the ranch by switching (manually) 17 of the lines from one board to the other. The detailed arrangement of the service is shown on the drawing. Provision has been made to install a switchboard on the ninth floor of the FOB if this should become necessary, but the board has not been installed.

The subscriber sets located at the ranch are of two general types - multiple (six) line call directors and single line sets.

In addition to the above there is:

~~SECRET~~

~~SECRET~~

-25-

- a. A small guard (police) station net at the ranch.
- b. A small guard (police) station net at the FOB.
- c. A vehicular (radio) service installed in various automobiles and connecting to the Bell service.
- d. A "party line" radio net which has numerous transmitters and receivers located at various ranches and in various vehicles, aircraft and helicopters.

2. Vulnerability of Texas system

Monitoring of conversations on the various systems described can be categorized as follows:

The "party line" network and vehicular services must be considered equivalent to a broadcast since receivers are available in the open market.

The telephone service, in general, is susceptible to monitoring. However, the microwave link from the ranch to Austin is the most vulnerable since a monitor could be located anywhere in the vicinity. The open wire carrier from Johnson City to Austin also presents a simple technical problem to monitor. The microwave and carrier require fairly sophisticated equipment not readily available on the open market. However, it can be built from available items by a competent technician or supplied by an agent. The commercial equipment is fairly large. However, miniaturized items have been built for use by the intelligence community.

Because of the length of the open wire carrier involved and the nature of the area, it is virtually impossible to inspect either visually or electrically for a clandestine tap or a listening post which could be located a considerable distance from the wire line.

Monitoring of circuits between Austin and, for example, Washington is of course possible, particularly as they appear in microwave. However, such monitoring is made difficult because of the diversity of circuits and circuit paths available. Thus a monitor would have to sift a lot of straw to find a few grains.

~~SECRET~~

~~SECRET~~

-26-

This type of operation might be conducted by an agent who was targeted on some other objective, e. g. , Bergston AFB and "lucked" into circuits used for Presidential service.

Since the ranch grounds and the ninth floor of the FOB are patrolled at all times, unauthorized monitoring or wiring changes by an agent would be difficult to accomplish; however, it is recommended that all terminal boxes be physically secured to prevent authorized access.

Because the various outlying houses and ranches are frequently completely unattended, it would be possible for an agent to gain access and install microphones and/or compromise telephones and then tap the cable. The establishment of such a tap and the associated listening post is practically rather difficult under the existing conditions in the area. However, telephones should be inspected periodically for compromises or other signs of tampering.

Calls to Washington can be monitored by operators and maintenance men.

~~SECRET~~

~~SECRET~~

VI. PROSPECTS FOR THE FUTURE

A. New Secure Voice Systems

A plan for increasing the amount of crypto-secured voice communications for the President is contained in the Defense Communications Agency Plan to Provide Communications for the President (January 7, 1965, revision).

The major immediate impact on voice communications in the near future will be the entry of the KY-3 and HY-2/KG-13 equipments into the inventory. Substantial numbers of KY-3 equipments will be available by the end of CY 1965 and should permit high-quality crypto-secured communications between the President and senior National Security officials.

The HY-2/KG-13 equipments will also be available in quantity by the latter part of CY 1965 and will permit secure service over long lines of a better quality than has hitherto been possible using the KY-9.

Currently, operational tests are under way of the KY-8, a tactical speech security equipment, which will permit encryption of mobile (car and helicopter) voice communications with at least minimum coverage in the latter part of CY 1965.

B. Improved Security in the White House

The present plans call for rewiring the White House with shielded cable so that the probability of pickup from between telephones will be reduced.

The special TEMPEST check which was started after the beginning of the study will lead to reduced probabilities of intercept of secure communications.

C. Possibility of a new switchboard

A new switchboard system is needed for the White House and the new executive office building. The plans for this board are not

~~SECRET~~

~~SECRET~~

-28-

yet complete. The Panel believes that inadequate attention has been given to the problem of security during the planning stage for the new board, and fears that if careful planning is not done there will be no possibility for major changes for many years.

D. Possibility of Digital carrier

A digital carrier system, such as the Bell T-1 Carrier system, makes eavesdropping more difficult and makes bulk encryption possible.

The T-1 Carrier equipment accepts 24 voice circuit, converts each channel into digital code and then combines the individual streams of pulses into a single stream. The receiver terminal separates the stream into 24 individual streams and then converts each stream of pulses into voice frequency signals.

The digital output (pulse stream) of the transmitting terminal can be encrypted by means of a single key generator and then decrypted at the other end by a similar key generator to provide crypto security over the portion of the link between key generators. The circuits from the subscriber to the T-1 equipment would, of course, not be secured cryptographically.

Unfortunately, the T-1 carrier equipment as now manufactured produces substantial compromising radiation and cannot therefore be approved for crypto-security.

Reducing the compromising radiation from the T-1 carrier is an expensive development which is still under consideration by BTL. These considerations are further complicated by the fact that BTL has currently under development the T-2 systems (functionally similar to the T-1, except that up to 24, 48, 72, or 96 channels can be stacked into one data channel).

The use of T-1 equipment without encryption would certainly pose a far more technically complex problem to an interceptor than the transmission of the same information over 24 wire circuits. The equipment required is of a complexity and type which would put it beyond the means of an amateur or casually curious. However, there is nothing required which cannot be built by a competent professional.

~~SECRET~~

~~SECRET~~

-29-

With encryption, the security would be entirely dependent on the quality of the key generator and the successful suppression of compromising radiations. Provision of a simple key generator which would be adequate for privacy does not seem to be possible for much less than the cost of providing a quality key generator. It is, therefore, possible that the use of a simple key generator might be desirable merely to preclude the compromise of more advanced principles through exposure in the telephone plant.

In any case, if a decision is made to utilize T-1 carrier with crypto a careful evaluation of the security criteria to be established for both ends of the link must be made.

~~SECRET~~

~~SECRET~~

TELETYPEWRITER SERVICE

SECURE

DEPT ARMY COMM CENTER
DEPT STATE COMM CENTER
DEPT NAVY COMM CENTER
DEPT AF COMM CENTER
DCA (OPN CENTER)
H. P.
AJCC
DAVID
EMBASSY (UK)
DIA
NMCC
INT. SIT. RM
CHALTENHAM RELAY STATION
ANDREWS AFB RELAY STATION
CIA (LANGLEY)
AIRPLANE
RANCH
(AND TO ALL POINTS VISITED
WHEN PRESIDENT IS IN
TRAVEL STATUS)

W.H. COMMUNICATIONS
CENTER

NON SECURE

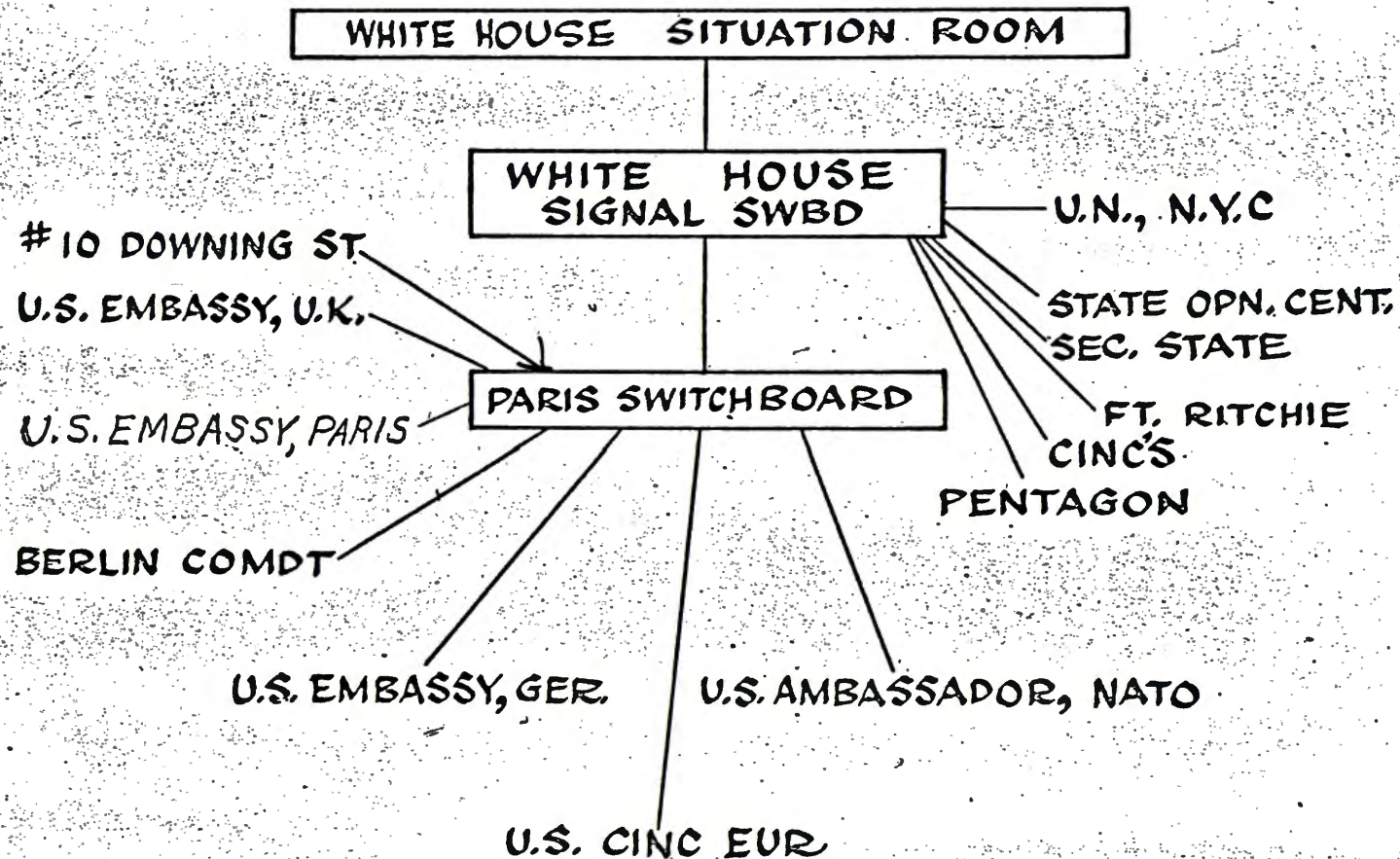
I.S.R.
MR. BUSBY OFFICE
TWX
NIAC

CIRCUITS TO ALL ARE OBTAINED
BY COMMERCIAL LEASES EXCEPT
THAT TO AJCC, H.P. PENTAGON
AND DAVID ALTERNATE ROUTES
ARE OBTAINED VIA GOVT OWNED
& OPERATED MICROWAVE

APPENDIX F- chart 1

~~SECRET~~

~~CONFIDENTIAL~~
SECURE VOICE LOW QUALITY



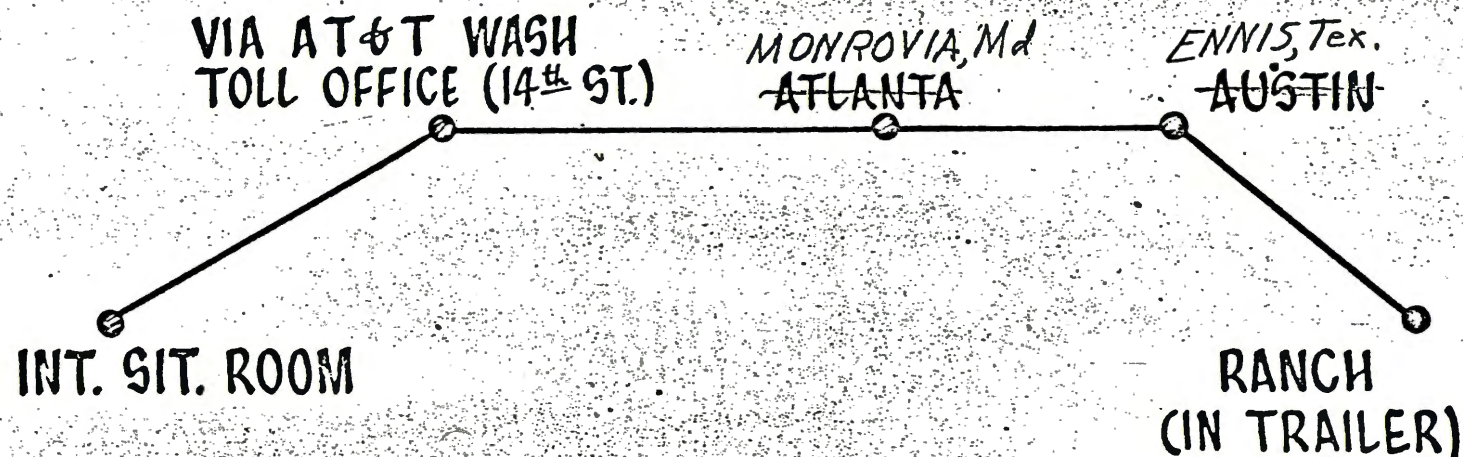
~~CONFIDENTIAL~~

(3)

~~SECRET~~

SECURE VOICE - WHITE HOUSE TO RANCH

POINT-TO-POINT HIGH QUALITY



~~SECRET~~

APPENDIX F Chart 3.

~~CONFIDENTIAL~~

HIGH QUALITY SECURE VOICE (IN TOWN)

AJEE
H P
DAVID
CIA (DIR & DUTY OFFICER)
AEC
1717 H. ST.
AEC GERMANTOWN
CHAIRMAN, JCS
ARMY WAR ROOM
NAVY FLAG PLOT

1. PRESIDENTS OFFICE
2. PRESIDENTS OFFICE (SHELTER)
3. W. WING SIT. ROOM
4. E. WING SIT. ROOM
5. SP. ASST. FOR INTEL.

SECURE VOICE SWBD
WHITE HOUSE

HIGH QUALITY
SECURE VOICE
(OUT OF TOWN)

SEC. STATE
SEC. DEF.
STATE OPNS.
N.M.C.C.
DIR. CIA.
(EAST BLDG.)

CIRCUITS INSTALLED BUT NOT EQUIPPED

VICE PRES. (CAPITOL) PRES. PRO. TEM. (SENATE)
SPEAKER OF THE HOUSE
SEC. AGRICULTURE SEC. TREASURER
SEC. INTERIOR SEC. LABOR
SEC. COMMERCE POST OFFICE

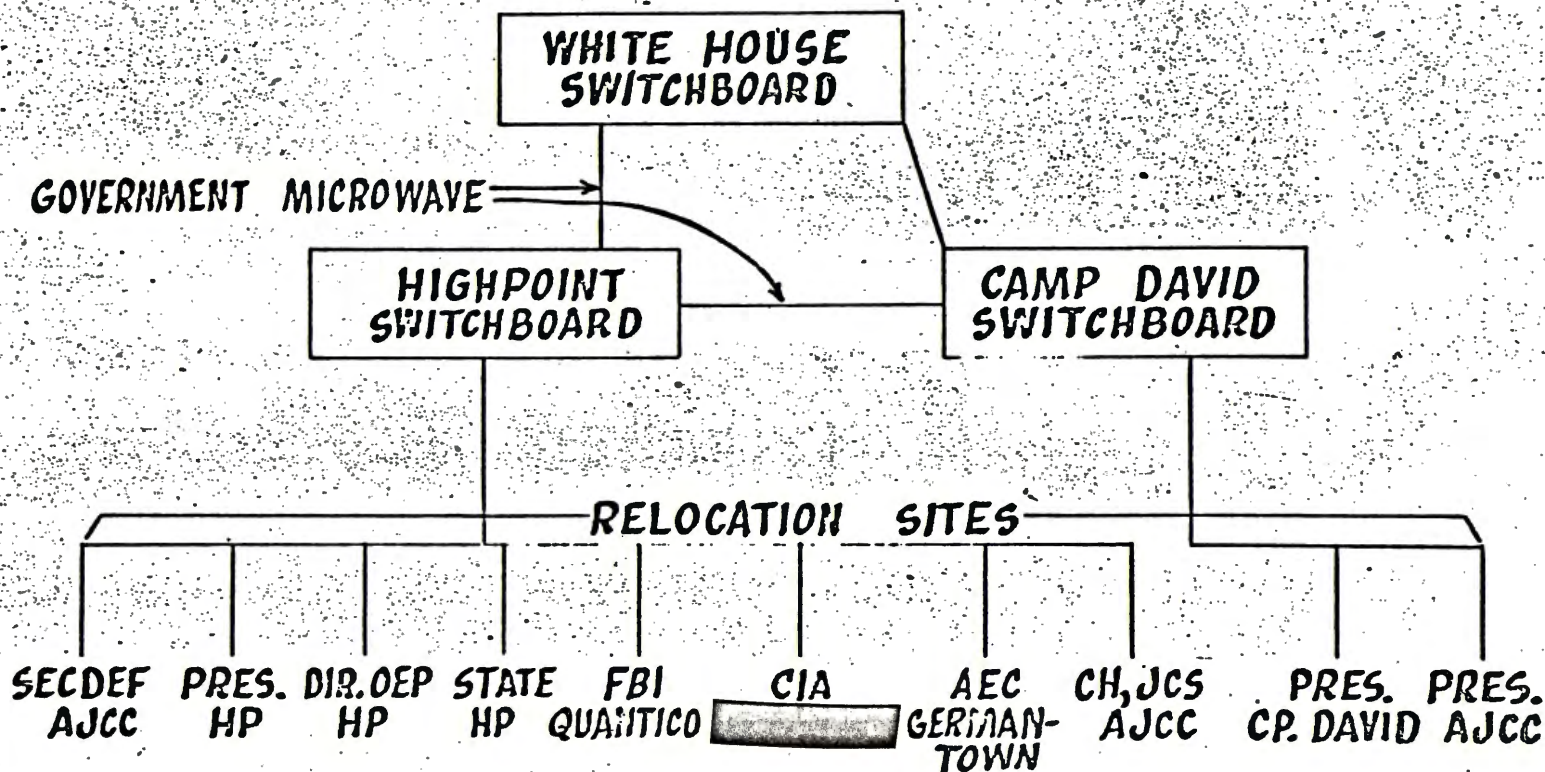
~~CONFIDENTIAL~~

*this should
be revised
to avoid confusion
The name has been
changed.
B1C9*

Appendix F Chart 4.

~~SECRET~~

OUT OF TOWN HIGH QUALITY SECURE VOICE NET



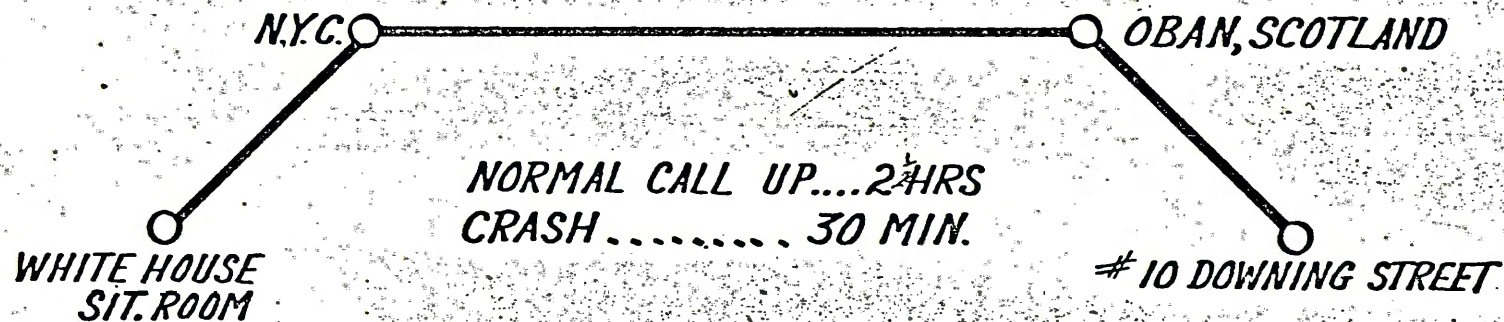
~~SECRET~~

APPENDIX F Chart 5.

~~SECRET~~

TWILIGHT NETWORK

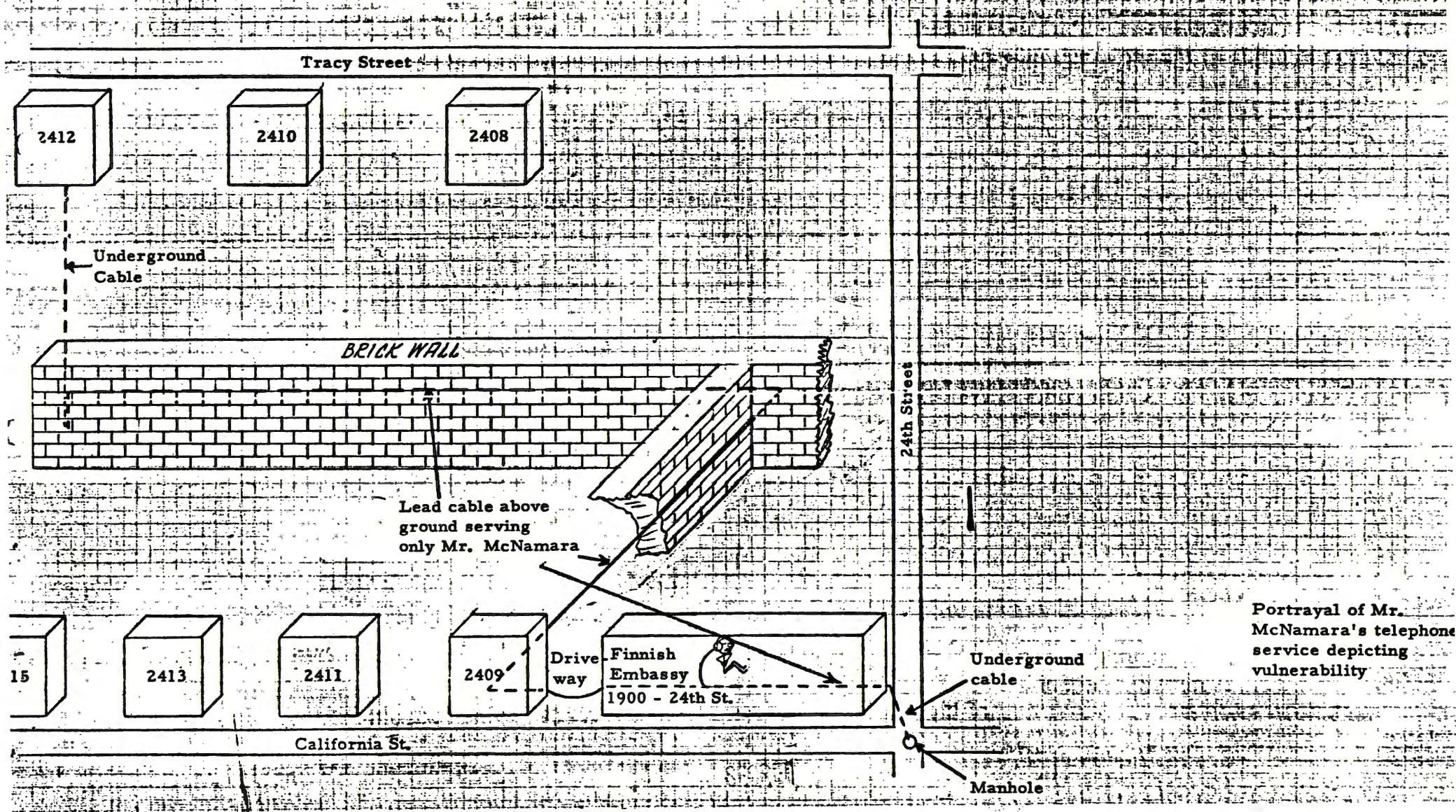
POINT TO POINT
HIGH QUALITY SECURE VOICE



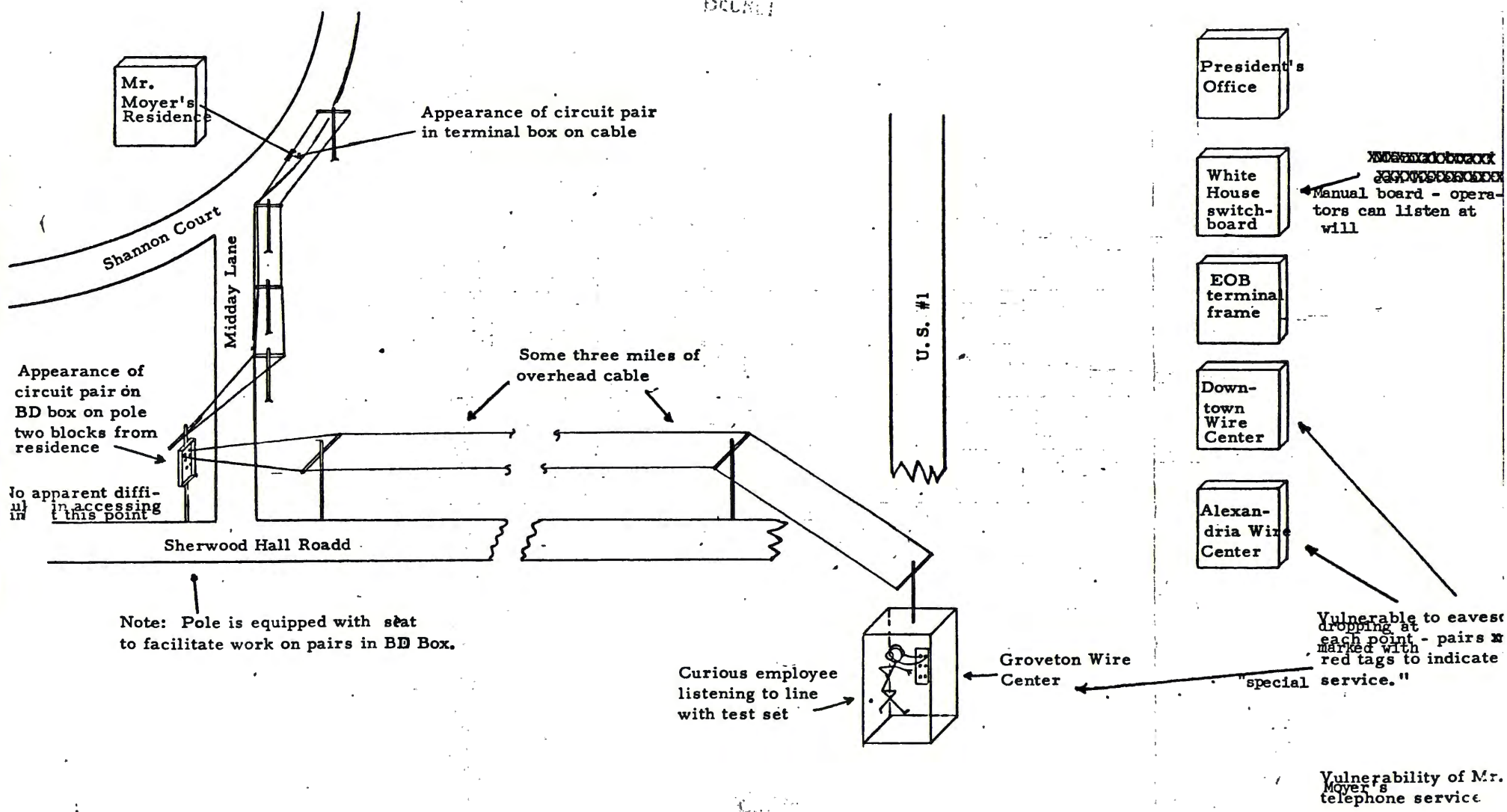
~~SECRET~~

Appendix F Chart 6.

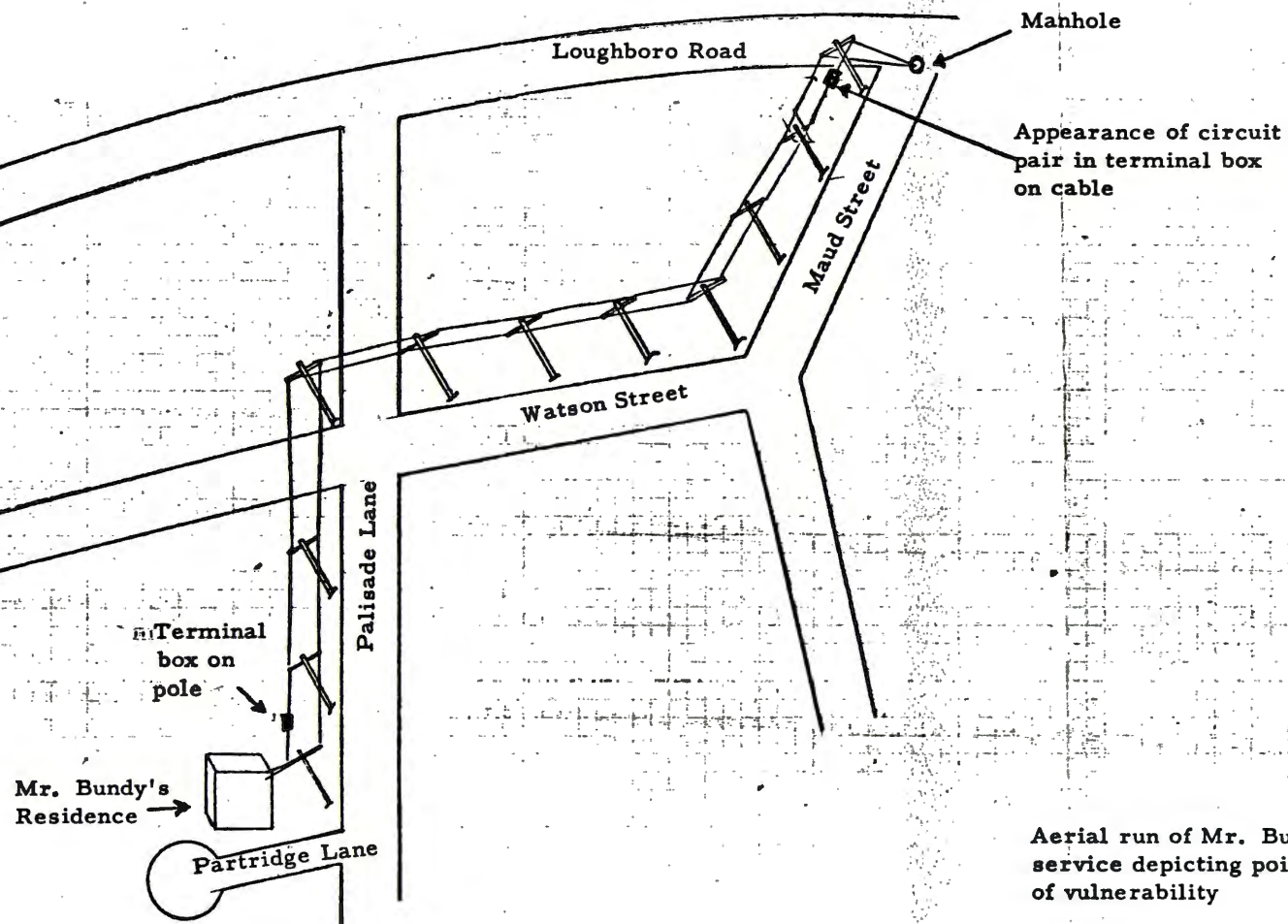
SECRET



SECRET



~~SECRET~~



Aerial run of Mr. Bundy's service depicting points of vulnerability

~~SECRET~~

~~SECRET~~

M-5B/65-S/6
C.8

\$
Chase

PANEL MEETING - MONDAY, MARCH 8, 1965

Consultants:

Jerome B. Wiesner	MIT
William O. Baker	Bell Laboratories
Edward M. David	Bell Laboratories
Richard James	AT&T

Study Group

James W. Clark	Assistant Division Chief (Air Force), Military Division, Bureau of the Budget
----------------	--

[REDACTED]
Leo Rosen

[REDACTED]
Assistant Director for Research and Engineering,
NSA

Raymond T. Tate

Chief, Radiation Engineering Section, Division
of Communications Security, NSA

[REDACTED]

Chief, Telephone Engineering Group, Office
of Telecommunications, NSA

David Z. Robinson

Technical Specialist, OST

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

G. Marvin Gentile

Deputy Assistant Secretary for Security, State

Joseph A. Califano, Jr.

Special Assistant to the Secretary of Defense

Spurgeon M. Keeny

Technical Assistant, OST

J. Patrick Coyne

Executive Secretary, President's Foreign
Intelligence Advisory Board

~~SECRET~~