UNCLASSIFIED

AD NUMBER
AD822597
LIMITATION CHANGES
TO: **Approved for public release; distribution is unlimited.**
FROM: **Distribution: Further dissemination only as directed by Office of Civil Defense (Army), Washington, DC, 31 JAN 1966, or higher DoD authority.**
AUTHORITY
OCD ltr 16 Sep 1971

THIS PAGE IS UNCLASSIFIED

AD822597

TM(L)-1960/091/00

Final Report for the Office of Civil Defense

Civil Defense Warning System Research Support

Volume II: Research Studies

31 January 1966

FOR OFFICIAL USE ONLY

TM-L-1960/091/00

TECHNICAL MEMORANDUM

(TM Series)

This document was produced by SDC in performance of contract OCD-PS-64-183
Work Unit Number 2212E

Final Report for the Office of Civil Defense

Civil Defense Warning System Research Support

Volume II: Research Studies

Special Research and Development Projects Staff

SYSTEM DEVELOPMENT CORPORATION
2500 COLORADO AVE.
SANTA MONICA
CALIFORNIA
90406

31 January 1966

OCD REVIEW NOTICE

This report has been reviewed in the Office of Civil Defense and approved for publication. Approval does not signify that the contents necessarily reflect the views and policies of the Office of Civil Defense.

AVAILABILITY NOTICE

This document has limited distribution and may be further distributed by any holder only with specific approval of OCD Research.

(Page ii Blank)

FOREWORD

Volume II, this Volume, and two companion Volumes contain the findings, conclusions, and recommendations resulting from the study of warning system requirements under contract OCD-PS-64-183. The three Volumes are as follows:

TM-L-1960/090/00
Final Report for the Office of Civil Defense
Civil Defense Warning System Research Support
Volume I: Radio Warning System Studies
31 January 1966

TM-L-1960/091/00
Final Report for the Office of Civil Defense
Civil Defense Warning System Research Support
Volume II: Research Studies
31 January 1966

TM-L-1960/092/00
Final Report for the Office of Civil Defense
Civil Defense Warning System Research Support
Volume III: Use of Damage Assessment Information for Warning (u)
31 January 1966

The Volumes were authored by the Special Research and Development Projects Staff composed of:

J L Autery
D. H. Kearin
R. L. Lamoureux
J. O. Neilson
M. I. Rosenthal
W. Stroebel
D. C. Swavely
S. Weems

CONTENTS

Page

CHAPTER 1: INTRODUCTION AND SUMMARY 1-1

CHAPTER 2: DECISION TO WARN 2-1

CHAPTER 3: LEGISLATIVE AND FISCAL HISTORY OF THE CIVIL DEFENSE WARNING PROGRAM 3-1

CHAPTER 4: STRATEGIC WARNING TO INDUSTRY 4-1

CHAPTER 5: RELIABILITY OF A GENERALIZED WARNING SYSTEM 5-1

CHAPTER 6: FEASIBILITY OF USING COMMUNICATIONS SATELLITES FOR PUBLIC ALERTING AND WARNING 6-1

Appendix A: Bibliography A-1

Appendix B: Glossary B-1

(Page vi blank)

LIST OF FIGURES

Figure		Page
5-1	Typical Fanout Network.	5-5
5-2	Series Combination of Components	5-22
5-3	Parallel Redundant Combination of Components	5-24
5-4	Condensation of Network Shown in Figure 5-1	5-26
5-5	Reliability Model for Warning System in Figures 5-4 and 5-5 .	5-28
5-6	Condensed Network of the Hypothetical National Warning Dissemination System (NWDS)	5-32
5-7	Reliability Model for NWDS	5-33
5-8	Reliability Worksheet	5-35
5-9	Completed Reliability Worksheet.	5-39
5-10	Warning System Jeopardy Analysis	5-45
5-11	Warning System Jeopardy Analysis	5-47

(Page viii blank)

LIST OF TABLES

Table		Page
5-1	States of Operation.	1-16
3-1	Warning Obligations - Fiscal Years 1951 through 1964	2-79
3-2	Comparison of Total Funds Requested and Those Appropriated vs. Selected Warning Funds Requested and Those Obligated	3-80
3-3	Obligation History of National Warning System (NAWAS and Predecessor Systems)	3-81
3-4	Obligation History of Washington Area Warning System (WAWAS).	3-81
3-5	Obligation History of Warning-Matching Funds	3-82
3-6	Obligation History of Emergency Broadcast System	3-83
3-7	Emergency Broadcast Systems: Other Government Agency Support	3-83
3-8	Obligation History of National Emergency Alarm Repeater (NEAR) System.	3-83
3-9	Obligation History of Radio Warning System	3-84
3-10	Obligation History of Fallout Protection for Warning Points	3-84
3-11	Obligation History of Warning Research and Development	3-84
5-1	States of Operation.	5-8
5-2	Failure and Repair Rates per Day for NWDS Components and Links	5-31
5-3	Relative Importance of Components	5-49
5-4	Required Reliabilities with Importance	5-50

CHAPTER ONE

INTRODUCTION AND SUMMARY

1.0 INTRODUCTION

In April 1964, the System Development Corporation (SDC) was awarded a contract (OCD-PS-64-183) by the Office of Civil Defense to continue activities in the area of civil defense warning system research support.

This volume and two others, TM-L-1960/090/00 and TM-L-1960/092/00 document and summarize the results of the research effort, and comprise the final report required by the contract.

The SDC staff performed the following tasks during the course of the contract:[1]

1. Assisted OCD in evaluating, selecting, and implementing a nationwide radio-based alert and warning system.

2. Selected optimum radio warning system configurations on the basis of operational and performance requirements and designated areas for detailed engineering study.

3. Determined, on the basis of operational and performance requirements, optimum signaling procedures to be used in the transmission and distribution elements of a radio-based alerting and warning system and studied the need for and degree of security of signaling and other related factors leading to the engineering design of signaling devices.

4. Studied the civil defense decision to warn at all levels of government--federal, state, and local.

5. Evaluated the feasibility and effectiveness of providing strategic warning to industry. Determined tradeoffs between shutdown of industry following strategic warning and possible escalation of a crisis versus no shutdown and probable damage to or destruction of plant and surrounding community. They also evaluated the impact upon federal warning systems and procedures if it appears feasible to provide such strategic warning for shutdown purposes.

---

1. Several other tasks were originally scheduled, but were not performed. These omitted tasks include a study of the optimum relationship between warning system development and shelter system development, an investigation of civil defense alerting conditions, and an analysis of improved processing of warning information at various civil defense operational levels. These tasks were omitted when other tasks undertaken under the terms of the technical support clause of the contract (Task 9, below) were assigned sufficiently high priority by OCD to necessitate reducing the overall scope of work.

6. Developed reliability criteria for evaluating both current and planned warning systems, including expressions for describing the levels of reliability at which a warning system will operate, and a mathematical model for the performance required of the improvements of any warning system if that system is to achieve a predetermined level of reliability.

7. Determined the degree to which federal warning programs have been accepted by the Congress; collected and assembled material showing the legislative and fiscal history of these programs; analyzed the development of the program in terms of the interaction of civil defense agency personnel with Congress; and traced changes in the nature of and the funding requested for program proposed as well as in the nature of and funding provided for programs accepted.

8. Determined the warning information that could be derived from a nuclear detection or damage assessment system; and reviewed and evaluated the warning potential of current, planned, and proposed nuclear detection and damage assessment systems.

9. Provided technical assistance and liaison on radio-based alerting and warning systems, and in other areas mutually agreed upon by OCD and System Development Corporation.

Volume II of the final report contains six chapters devoted to the findings of research studies (Tasks 4 through 7, and 9, above), a Bibliography and a Glossary. The chapters are devoted to the following subjects:

- Chapter One, Introduction and Summary: Contains an introduction and a series of summaries of the succeeding chapters of this volume.
- Chapter Two, The Decision to Warn: Analyzes the decision to warn at the national level.
- Chapter Three, Legislative and Fiscal History of the Civil Defense Warning Program: Examines the development of the civil defense warning program.
- Chapter Four, Strategic Warning to Industry: Discusses the tradeoff between shutting down and not shutting down industry in a crisis.

- Chapter Five, Reliability of a Generalized Warning System: Provides a theoretical background for establishing reliability requirements for warning systems still in conceptual stages and for evaluating the performance of warning systems already deployed.

- Chapter Six, Feasibility of Using Communications Satellites for Public Alerting and Warning: Discusses the capabilities of currently operational or planned satellites and evaluates their use for public alerting and warning.

Chapters Two through Six reproduce previously published reports. However, they have been updated, where necessary, to reflect the status of the Radio Warning Program as of 31 January 1966. No attempt has been made to provide continuity from chapter to chapter.

Volume Two, TM-L-1960/091/00, contains the findings of all other unclassified warning research studies. These include Tasks 1 through 3, and 9, above.

Volume Three, TM-L-1960/092/00, is classified Secret Restricted Data. It contains information warning data that could be derived from a nuclear detection or damage assessment system (Task 8, above).

Sections 2.0 through 6.0 below summarize Chapters Two through Six, respectively, of this volume.

2.0 SUMMARY OF CHAPTER TWO: THE DECISION TO WARN

The warning process consists of many phases, including the entire sequence of actions from threat perception, to the decision to warn, to warning dissemination, and finally to completion of the protective reaction. The "Decision to Warn" focuses on the warning decision at the national level, and as such investigates the first two phases--the intelligence phase (data input, analysis, and evaluation) and the decision phase.

The investigation of the warning decision process can be subdivided into several parts determined by the type of threat. During the "normal," low-level, threat that we usually experience from day to day no decision to warn is necessary. The news services keep the public apprised of current international events. When these events erupt past the established control processes the public is informed through the release of crisis information. Here the object is to make people aware of the crisis situation, not to direct them to do anything about it. Crisis information is disseminated either through commercial news facilities or by means of Presidential and other official broadcasts over radio and television.

A second type of public awareness to a threat can be disseminated by a Presidential declaration of a strategic warning. Here the public is directed to take some action for their own protection prior to the detection of an actual attack. Strategic Warning requires a Presidential decision to warn and a Presidential announcement of the warning.

A third type of public awareness to a threat, tactical warning, is based upon the detection of an actual attack. If the detection has been made and evaluated NORAD declares an Air Defense Emergency and OCD personnel at the National Warning Center (NWC) respond automatically by implementing the tactical warning. In this case the decision to warn has been made far in advance of the need and the warning is disseminated after a set of predetermined conditions have been met.

The function of determining whether to warn, how to warn, and when to warn is the warning decision process. This process separates quite naturally into two phases: 1) the intelligence phase, and 2) the decision phase. Throughout the intelligence phase of the warning decision process there are successive stages of data gathering, analyzing, evaluating, and synthesizing. Agencies such as the Central Intelligence Agency, Joint Chiefs of Staff, State Department, Federal Bureau of Investigation, and Department of Defense gather threat information, synthesize it into threat intelligence, and forward it to the National Security Council. It is at this level that threat intelligence is presented to the President, and, in light of the current defensive posture, recommendations on alternative courses of action are made.

Most Presidents maintain a small group of trusted advisors with whom they can confer during crises. During the Cuban Missile Crisis of 1962, President Kennedy formed the National Security Council Executive Committee (Ex Comm). President Johnson has formed his own compact "Kitchen Cabinet" consisting of McGeorge Bundy, Robert McNamara, and Dean Rusk. The formal and informal groups of advisors aid Presidents in formulating their decisions, but the decision remains that of the President alone.

The posture of our military and civilian readiness to meet a given threat will greatly influence the timing, content, and method of dissemination of crisis information, strategic warning, or tactical warning. Military readiness is a function of our defense philosophy and the operational readiness of our forces. Civilian readiness, unlike the military readiness which is structured to maintain a relatively high level of preparedness at all times is a varying condition. This is so because civil defense is composed of two aspects, their compatibility being a somewhat fluctuating thing: 1) the program which the federal government provides for survival, and 2) the public awareness of the program and how prepared the people are to take advantage of it.

Strategic warning may be the outcome of the consideration of the threat versus the military and civilian readiness. The United States, however, has never employed strategic warning. The 1962 Cuban Crisis produced crisis information; the Japanese attack on Pearl Harbor produced tactical warning but we have never had strategic warning.

The strategic warning decision point was approached during the 1962 Cuban missile crisis when President Kennedy informed the public of the threat and the action initiated to counter it, but stopped short of directing the public into action.

Surprise attack by the major powers seems unlikely during the foreseeable future. The balance of power is such that either side would suffer losses of such enormity that other means of advancing national policy may be more desirable than war. Tactics that use some form or combination of limited strikes, blackmail, manufactured crises, subversion, etc., have been used with varying degrees of success since World War II without the result of a major war. We might, then, expect a continuation of these tactics in preference to a direct attack on the United States either following a strategic buildup or as a surprise.

Tactical warning is the giving of official direction to the people to take certain precautionary measures to protect themselves as a result of the direction of an actual hostile attack against the continental United States. The attack could follow a period of crisis and strategic build-up, or it could, although unlikely, occur unexpectedly. In either case the detection, evaluation, and dissemination of tactical warning would have to be accurate and swift. A time constraint exists during the tactical situation, not present during the strategic situation, that necessitates the need for formal, predesigned warning procedures and the requirement to evaluate their effectiveness. These procedures define the conditions for intiating tactical warning based upon the general national grand strategy of defending ourselves if attacked. Defense of our population, government, industry, and military capabilities depends, in part, upon the amount of warning time the country receives. A vast air defense system has been devised and made operational to provide the greatest warning time possible so that the nation can react positively to the threat. Many contingencies of an attack have been anticipated, and the air defense system has been exercised utilizing the contingency situations. Methods of reacting to a variety of attacks have been devised and the decision to react automatically, in a prescribed manner, has been made. This study, therefore, considers the tactical warning decision, occurring at the time of attack, as a subprocess, i.e., the implementation of previous decisions.

The federal government, primarily through the Department of Defense is charged with the responsibility of detecting and recognizing an imminent attack, either before or soon after it has been launched. The North American Air Defense Command, concurrent with the Continental Air Defense Command, has operational control of the personnel, facilities, and weapons of four component service commands to carry out its mission of the air defense of North America. These commands are:

1. USAF Air Defense Command (ADC)
2. U.S. Army Defense Command (ARADCOM)
3. Naval Forces NORAD Command (NAVFORNORAD)
4. Royal Candian Air Force - Air Defense Command (RCAF - ADC)

NORAD headquarters, located in the NORAD Combat Operations Center (COC) at Colorado Springs, Colorado, and an alternate operations headquarters (ALCOP) are the central receiving points for tactical information. Lesser quantities of tactical information of a local nature come to the NORAD COC from NORAD Region and Sector command centers. The other seven unified and specified commands are capable of making tactical data inputs from attacks on their components.

Tactical inputs in the form of air breathing vehicle detection, missile detection, space object detection, submarine detection, and nuclear detonation detection are used as basic information for threat evaluation. These inputs are received in the NORAD COC. Evaluators in the COC are needed to study the inputs, analyze and synthesize the data, and present the evaluation of the threat to the decision-makers for their consideration of appropriate action.

NORAD has the capability of judging the implications of the data it gathers and evaluates. It knows the system's limitations and its capabilities. There are other decision-making centers, such as the Joint War Room, SAC Headquarters, and the White House that receive threat information directly from some of NORAD's threat input sources. They may also have some unevaluated data automatically transferred to them through the NORAD COC. However, NORAD is the only area that has direct access to all unevaluated data plus the experienced men and equipment necessary for data evaluation.

NORAD's detection and evaluation system provides the intelligence from which NORAD Commanders determine the probability or imminence of air attack. The tactical information available on the various displays at the NORAD COC includes quantitative estimates of the threat, communications status, and the status of defensive forces. OCD National Warning Center (NWC) personnel have access to all of these data. In addition, they participate in intelligence briefings and have a drop on CINCNORAD's internal tactical phone. In essence, they have the same information available to them as do NORAD threat evaluation personnel.

The NWC personnel use the intelligence information, the military situation, command decisions within the NORAD COC, existing OCD directives, and the status of communications as the basis for carrying out their mission. That mission is to declare the Air Raid Warning and transmit it to the civilian population of the United States.

The decision to warn the public of a tactical threat is made at the national level. In effect, it is a decision that has already been made.[1] The Office of Civil Defense has written directives and established standard operating procedures for the declaration and dissemination of Air Raid Warning. Unlike the decision to give strategic warning which would or would not be made by the President during a critical situation, the giving of tactical warning is dependent upon the existence of certain predetermined conditions. Thus, it has already been decided that if these conditions exist, namely, that an attack has been launched against the United States or that the Country has been hit by hostile forces, tactical warning will be declared. The role of the OCD Warning Officer at the NWC is not to decide whether to warn or not to warn; rather, it is to implement the foregone decision. Thus, upon the NORAD declaration of an Air Defense Emergency, the OCD Warning Officer immediately and automatically responds by declaring Air Raid Warning.

The greatest effort of the OCD personnel in the tactical warning process is in its final phase, that of implementing the decision to warn.

3.0 SUMMARY OF CHAPTER THREE: LEGISLATIVE AND FISCAL HISTORY OF THE CIVIL DEFENSE WARNING PROGRAM

Chapter Three, which examines the development of the civil defense warning program, is intended as a resource document for future warning studies. It performs the following functions:

1. Collects material showing the legislative and fiscal history of the civil defense warning program.

2. Analyzes the development of the civil defense warning program. Emphasis is placed upon the verbal and fiscal interaction of the federal civil defense agencies with various Congressional committees (especially the Independent Offices Subcommittee of the House of Representatives).

---

1. As a result of the reassignment of the OCD communication-electronics functions to the U.S. Army Strategic Communications Command (STRATCOM), the responsibility for disseminating civil warning is now formally vested in the hands of a military organization, even though all warning officers are civilians and employees of STRATCOM.

3. Details the development of the civil defense warning program, showing the nature of and requested funding for programs proposed as well as the manner in which these proposals were made; the nature of and funding provided for programs accepted as well as any identifiable Congressional response to the initial proposals.

3.1 CONCLUSIONS

Funding of the Civil Defense Warning System, with the possible exception of research efforts, has received adequate and consistent Congressional support throughout the program's history.

It is considered that this support can be traced to three basic factors:

1. The original program was an extension of one started by the military which already had Congressional support.

2. There were no radical changes in program direction from year to year. Rather, the proposals made provided for orderly growth of the system. Thus, Congress was able to judge what was proposed against what had been accomplished.

3. About 40 percent of the funds were for direct support of the state and local effort.

3.2 GUIDE TO ANNEXES

Annex I to this chapter (pp. 3-12 ff) covers pertinent excerpts from the hearings on authorizing legislation; Annex II (pp. 3-15 ff) covers hearings on the status of civil defense; and Annex III (pp. 3-20 ff) covers hearings on the annual appropriations for civil defense. Annex IV (pp. 3-79 ff) covers the fiscal history of civil defense warning systems including a summary of total obligations by major warning programs for fiscal years 1951 through 1964; a comparison of selected warning funds requested and those obligated versus the total funds requested and those appropriated; and a year-by-year analysis of funds obligated by the warning program.

3.3 DEVELOPMENT OF THE CIVIL DEFENSE WARNING SYSTEM

Over the years, a number of subsystems of the warning system has been separately justified and funded. In this report, each subsystem is traced from its inception. The subsystems are:

National Warning System (NAWAS)
Control of Electromagnetic Radiation (CONELRAD)
and its replacement,
The Emergency Broadcast System (EBS)
National Emergency Alarm Repeater (NEAR) System
Radio Warning System.

3.3.1 National Warning System

Included in this discussion is the system for the transmission of attack warning intelligence from the federal to the state and local levels, and the program for providing financial assistance to the state and local levels for the outdoor warning system.

Work on a national warning system was initiated immediately upon establishment of the Federal Civil Defense Administration in 1950. In the hearings on the authorizing legislation, once certain questions were clarified for the committee members, the program received Congressional support (Annex I. pp. 3-12 ff). Included in the chapter are data that enumerate funds requested and funds appropriated for the National Warning System program from fiscal year 1951 through 1965.

Except for fiscal year 1951, when the action of the congress in denying funds apparently was due to a misunderstanding of the program, the federal warning system and the program to provide matching funds for warning purposes have received excellent financial support from the Congressional committees as compared with the support afforded other programs (Annex IV, pp. 3-79).

3.3.2 National Emergency Alarm Repeater (NEAR) System

The first actual discussion of the NEAR system occurred in the appropriations hearings for Fiscal Year 1962 (Appendix III, pp. 3-48 ff). Data is presented in the chapter regarding NEAR's history of Congressional support up to the abandonment of the system in 1966. Total expenditures amounted to $8.5 million, including research costs.

3.3.3 Radio Warning System

In Fiscal Year 1959, $800,000 was requested in research and development funds for determining the most favorable means of communicating with the people via standard broadcasting stations (Annex III, pp. 3-40ff). The House did not allow the funds and in the Senate hearings, the civil defense witness indicated that the cut was not being appealed (Annex III, pp. 3-41 ff).

During the following years there were occasional questions raised regarding the possibility of using radio as a warning device, but no indication of the feasibility of utilizing such a system was given until the hearings on the 1965 appropriations. In the House hearings for 1965, a number of possibilities for

utilizing the radio for warning was discussed. The civil defense witness indicated that by the end of Fiscal Year 1965, $1.6 million would have been spent on the final look at the radio warning system.

In the House hearings on the 1966 appropriation, the civil defense witness indicated that technological reports indicated the Radio Warning System to be feasible, and that they were working with the FCC and radio broadcasting industry on the project. However, no funds for 1966 for this purpose were requested.

3.3.4 Control of Electromagnetic Radiation (CONELRAD) and the Emergency Broadcast System (EBS)

From its inception in 1951, there was very little Congressional questioning regarding the CONELRAD program or its financial support. In the Fiscal Year 1962, House hearings on appropriations for the Federal Communications Commission, Commissioner Lee indicated that, in his judgment, CONELRAD was the "most important and realistic part of the whole civil defense program" (Annex III, p. 3-47). Late in Fiscal Year 1962, the program for hardening selected broadcast stations was begun. Some 50 stations were so hardened during the year.

In March of 1963, the FCC's National Industry Advisory Committee recommended the Emergency Broadcast System (EBS) to replace CONELRAD. EBS would permit the stations to broadcast at normal power at normal frequencies. The EBS was implemented on August 5, 1963.

Funds in the amount of $2 million were requested in Fiscal Year 1966 to complete the national coverage requirement of 658 stations.

4.0 SUMMARY OF CHAPTER FOUR: STRATEGIC WARNING TO INDUSTRY

This chapter presents the preliminary findings of the study on providing strategic warning to industry. The objective was to determine the time requirements and costs involved in an emergency shutdown, the feasibility of providing strategic warning to industry, and tradeoff between shutting down and not shutting down industry in a crisis situation. The potential consequences of a strategic warning false alarm were also considered in the study.

4.1 CONCLUSIONS AND RECOMMENDATIONS

1. Estimates of shutdown time requirements indicate that shutdown could not, in a number of significant cases, be accomplished within the time constraints of a tactical warning. Since many key industries would be self-destructive if merely abandoned and not shut down, then warning and shutdown procedure must be developed to maximize the survivability of those industries not directly affected by an attack.

2. The feasibility of giving industry strategic warning is dependent upon the level of civilian defensive preparedness. Thus, considering the low level of civilian preparedness today, it does not appear feasible to give industry strategic warning without first building the public's awareness of an impending threat.

3. No formal communication channels presently exist from the federal government to industry over which a strategic warning could be disseminated.

At this time only a very general recommendation can result of this effort. Therefore, a more comprehensive study should be made of key industries to determine more specifically the feasibility of providing strategic warning to industry, and the risks to industry and the surrounding communities of not responding to a warning to shut down versus the cost and consequent liabilities of a shutdown.

4.2 METHOD OF APPROACH

In accomplishing the task, a survey was conducted of five representative key industries:

1. Jones and Laughlin Steel Corporation, Pittsburgh, Pennsylvania

2. General Foods Corporation, White Plains, New York

3. Standard Oil Company of New Jersey, New York, New York

4. American Cyanamid Company, Wayne, New Jersey

5. Chase Manhattan Bank, New York, New York

Representatives of each industry were interviewed to obtain the following information:

1. Estimates of time required for normal accelerated, and maximum speed shutdowns.

2. Physical and economic consequences to a plant of a maximum speed shutdown, and of failing to shut down.

3. The degree to which shutdown could progress before it became common knowledge to plant personnel and the surrounding community, and the extent to which a skeleton crew could maintain operations in the plant in the event of an attack.

4. The type and source of information now available to industries during a crisis.

Additional information was sought by means of written survey forms. Since the written response was limited, information was sought from the General Electric Company to provide a better basis for analysis. Data on actual emergency shutdowns were also used.

4.3 DEFINITION OF INDUSTRIES

For the purpose of analysis, the industries studied were grouped into three general categories according to the kind of operation in which they are involved:

1. Operational - a functional or service entity whose activities are concerned primarily with inventory manipulation and/or record processing. A bank falls into this category.

2. Discrete Production - an industry concerned primarily with manufacturing. Activities involve only a few production steps or the assembly of finished parts into a particular item, or can involve both machinery and limited processing. A jet engine factory falls into this category.

3. Continuous Production - an industry characterized by activities involving complex multistage production processes. An industry falling into this category would be a chemical company.

4.4. SHUTDOWN TIMES

The minimum time required for a total nondestructive shutdown which would allow complete safe abandonment ranged from 20 minutes for a bank to 20 hours for an oil refinery. The minimum time required for a total shutdown without regard for plant safety ranged from 20 minutes to four hours.

4.5 SHUTDOWN COSTS

Costs for a total, nondestructive shutdown depend upon the size and kind of operation, and range from negligible to an estimated $100,000. The biggest single cost factor would be in loss of profit from production stoppage. The cost concerns for a total shutdown without regard for plant and/or equipment destruction ranged from negligible to $200,000,000. The cost factors here would involve both production profit losses and plant and equipment damage from fire and explosion.

The complete abandonment of a plant without shutting down would be very costly, could be disastrous, and would be an almost untenable alternative.

4.6 PARTIAL SHUTDOWN

Partial shutdown and the continuance of limited operations, though not considered practical for either the operational or discrete production industry, are very desirable for the continuous production industry. The time required for such a shutdown is high, but shutdown and start-up costs would be cut in half, and equipment and inventory losses would be negligible.

4.7 THE CONCEPT OF INDUSTRIAL WARNING

In determining whether or not to give industry strategic warning, there are many questions to answer: Is the concept feasible? What are the consequences to giving it, and not giving it? These and many other questions must be answered.

4.7.1 The Requirement for Industrial Warning

Considering the allowable reaction time to a tactical warning--15 minutes to a half-hour in target areas--it can be seen that neither a total non-destructive shutdown nor a total shutdown without regard for plant survivability could be accomplished within this time frame. The only alternative appears to be total abandonment. It has been pointed out, however, that equipment and complex processes will, if left unattended, eventually destroy themselves and their entire surroundings. If the effect of a hostile attack upon the nation's industrial capability is to be minimized--and it must if the nation's economy is to survive--then industrial facilities in areas not directly affected by the attack must not be allowed to add to the general destruction through their inability to terminate operations in a safe manner. Effective warning and shutdown procedures must be designed.

4.7.2 Feasibility of Industrial Warning

Industry is the public. A warning to industry is a warning to the public. The feasibility of giving industry strategic warning is dependent upon how the public would respond.

In a threat situation, the public's concern about the crisis can be expected to grow. People will seek information and direction, and without being told anything officially, will tend to accept any word, even rumor, as the truth and will react to it as they interpret it. If the public were at a high level of civilian preparedness and knew what they should be doing to protect themselves, reacting to such things as rumors would not be a problem because they would at least be going in the right direction. But, if the civilian defensive posture is low, reaction to rumor cannot always be predicted, therefore the reaction to an industrial strategic warning could be chaotic.

Considering the general low level of civilian preparedness which prevails today, it does not appear feasible to give strategic warning to industry without first building the public's awareness of an impending threat.

In addition to the problem of public reaction to an industrial strategic warning, there are no formal communications channels over which such warning could be disseminated. Informal channels exist over which some industries keep attuned to a crisis, but the concern generated by the threat is usually from the standpoint of how profits might be affected, not survival.

4.7.3 Cost Considerations

From the standpoint of industrial survival, cost is not a consideration. In determining how and when an industrial strategic warning might be given, there are many peripheral costs which must be considered.

In a total non-destructive shutdown, production profit losses are considered the largest single cost. The second most significant cost is start-up and equipment damage. Based upon the estimates received, these costs on a national scale could easily amount to a billion dollars. If the nation's industry actually shut down and thus survived a hostile attack, these costs, as great as they might be, would actually be of little consequence. If, however, an industrial strategic warning was issued and industry did shut down, but the attack did not materialize, of what consequence would these costs then be? Who would be liable for this false alarm? Of what consequence to the national economy would a total demobilization of industry be?

4.7.4 Additional Considerations

The consequences of a false alarm industrial strategic warning would probably be most obvious from an economic standpoint, but there are other factors--if the warning precipitated an enemy attack, the public faith in the credibility of warning would be undermined, what to do with the millions of people released from work--which would weigh heavily upon any decision to give it.

Not to give strategic warning in the face of a threat could be suicide should the attack materialize; but, to give it and have the warning turn out to be a false alarm could spell disaster of a magnitude not yet fully contemplated.

5.0 SUMMARY OF CHAPTER FIVE: RELIABILITY OF A GENERALIZED WARNING SYSTEM

The purpose of this chapter is twofold: 1) To provide a theoretical background for the establishment of reliability requirements for warning systems still in the conceptual stage; 2) To present the rationale for optimal system testing, given the reliability functions for the system. The approach is to provide "building blocks," from which any warning system can be modeled for reliability

purposes. No consideration is given to the timeliness of warning or the individual's response to a warning. All results are couched in terms of the number of components effected by either the receipt of a false warning or the failure to receive a valid warning.

5.1 CONCLUSIONS AND RECOMMENDATIONS

This study shows that from the basic reliability data available (or assumed) on the components of a warning system, it is possible to develop, in a statistical sense, the operating characteristics of that system in terms of components effected by false alarm and no alarm failures; the expected number of false alarm and no alarm situations; and the expected durations of these situations. While these do not, of course, tell the whole story of the system effectiveness, they do give an indication as to how well it will satisfy the needs of the public and the warning agency.

In the area of work to be done in reliability of warning systems, the establishment of rigid standards is mandatory. Just what is an acceptable number of false alarm or no alarm failures per year? What is the minimum requirement for system performance measure? What is the maximum number of hours of downtime per year per terminal warning device acceptable for adequate warning? These questions are in effect variations of the fundamental question: What percentage of the population may be put at risk because of either kind of system failure? This question and its derivatives must be answered even by command decision, if necessary. Theoretical studies cannot evaluate human beings in mathematical terms.

A second area requiring exploration is the relationship between cost effectiveness and reliability. This would mainly be a study of sophisticated components versus cheap, redundant components in their overall effect on system performance.

By computerization, and Monte Carlo techniques, it is possible to gather distributional data rather than averages as in this study. Rather than assume a symmetrical system, it is possible to distribute realistically the various warning dissemination levels with respect to the population, and, even more importantly, adjust the various failure rates to correspond, for instance, to the seasonal variations in noise levels in radio links, or to the population distribution with respect to day and night situations. With these adjustments, the model could then be run and reasonable distributions derived for the percentage of population in jeopardy for various situations.

However, even in its present form, the methodology developed in this chapter finds definite application to such developmental studies as the Decision Information Distribution System (DIDS) and the Radio Warning System, as well as such existing systems as the National Warning System (NAWAS) and the Washington Area Warning System (WAWAS).

5.2 CONCEPTS AND DEFINITIONS

A warning system is defined as a collection of entities capable of disseminating warning from the originator to the ultimate recipient of the warning. A subsystem is any clearly identifiable portion of the system capable of receiving and/or disseminating further the warning message. A warning device is a special subsystem used to disseminate the warning to the ultimate recipient. A component of a warning system is the smallest assemblage of elements that is capable of disseminating warning. Reliability is defined as the measure of system (or subsystem) availability and response, i.e., the probability that the system (or subsystem) will be able to perform its assigned function when called upon to do so, and not otherwise. This definition recognizes both false alarm and no alarm failures as system failures. By knowing the population distribution with respect to warning devices, it is then possible to determine, in a statistical sense, the proportion of the population that will be placed in jeopardy because of lack of warning or false warning.

The following constraints apply to this study:

1. It is restricted to maintained systems operating in a steady state, i.e., operating long enough that the failures are random in nature and not the result of breaking in or turning on the systems.

2. No attempt is made to determine the effects of sabotage on any portion of the system.

3. It is assumed that the generalized system is a fanout system without loops, i.e., the system is similar in overall structure and function to that existing in the current civil defense warning system, or to that proposed for the National Emergency Alarm Repeater (NEAR) System or the Radio Warning System.

5.3 COMPONENT RELIABILITY PARAMETERS

This study is specifically concerned with investigating a generalized component with the states of operation (or nonoperation) given in Table 5-1.

Table 5-1. States of Operation

State	Meaning
P_0	The component is operating in a satisfactory manner.
P_1	False alarm state; the component is operating when it should not be.
P_2	No alarm state; the component is not operating when it should be.

In order to discuss the transition probabilities from one state to another, a transition matrix P is constructed. Given that a is the rate of false alarm failures per unit time for a component (or a system), and b is the rate of no alarm failures, then the probability of the equipment remaining in operation (state P_0) during the time period from t to t+dt is 1-(a+b)dt, the probability of failing on (state P_1) is adt, and the probability of failing off (state P_2) is bdt. If the rate of repair of failed equipment is m, then the probability that a piece of equipment already failed into either state P_1 or P_2 will return to the operational state P_0 in the period from t to t+dt is mdt The transition matrix shows the probabilities P_{ij} of going from state P_i at time t to state P_j at time t+dt where i denotes the row number of the matrix and j denotes the column-number.

$P(t) =$

	P_0	P_1	P_2
P_0	1-(a+b)dt	adt	bdt
P_1	mdt	1-mdt	0
P_2	mdt	0	1-mdt

To make these transition probabilities meaningful, in a reliability sense, to this examination, the matrix must be converted into a series of equations such that the probability of being in a given state is given as a function of time, t, from the beginning of component operation. The procedure is as follows: the probability that the component is in state P_0 at time t+dt is the sum of three probabilities that express the three mutually exclusive ways in which the equipment can arrive in that state: 1) the equipment was already in state P_0 at time t with probability $P_0(t)$ and remained in that state until t+dt with probability 1-(a+b)dt; 2) it was in state P_1 at time t with probability $P_1(t)$ and returned to state P_0 (i.e., was repaired) at time t+dt with probability mdt; or 3) it was in state P_2 at time t with probability $P_2(t)$ and returned to state P_0 at time t+dt, also with probability mdt. The probability

that the component was in state i at time t and moved to state j at time t+dt is expressed as the product of the separate probabilities of 1) being in state i at time t and 2) of moving to state j at time t+dt. Therefore, the probability of being in state P_0 at time t+dt can be expressed as follows:

$$(1) \quad P_0(t+dt) = P_0(t)\ [1-(a+b)dt] + P_1(t)mdt + P_2(t)mdt$$

Similarly it can be shown that the probabilities of being in states P_1 or P_2 at time t+dt can be expressed as:

$$(2) \quad P_1(t+dt) = P_0(t)adt + P_1(t)(1-mdt)$$

$$(3) \quad P_2(t+dt) = P_0(t)bdt + P_2(t)(1-mdt)$$

In order to remove the variable t+dt from equations (1)-(3), employed is the definition of the differential of a function

$$P_i'(t) = \frac{P_i(t+dt) - P_i(t)}{dt}$$

where the prime indicates the differential with respect to time. Some rather mathematical manipulations result in the following expressions which give the probability that a component will be in any given state assuming that it is in steady state operation:

$$P_0(\infty) = P_0 = \frac{m}{a+b+m}$$

$$P_1(\infty) = P_1 = \frac{a}{a+b+m}$$

$$P_2(\infty) = P_2 = \frac{b}{a+b+m}.$$

By further manipulations, it is possible to determine that the mean time to first failures (MTTFF) is

$$(MTTFF) = \frac{1}{a+b}$$

The mean time to first failure for a false alarm MTTFF(1) is

$$[MTTFF(1)] = \frac{1}{a}$$

The mean time to first failure for no alarm MTTFF(2) is

$$[\,MTTFF(2)\,] = \frac{1}{b}$$

and the mean time to repair [MTTR] is

$$(MTTR) = \frac{1}{m}$$

What has been presented so far applies to a component only during its initial operating phase before its first failure. The operating characteristic of the component during a given time period 0 to T, in which it might fail and be repaired several times, can be explored through the use of renewal theory. This will provide the expected number of repairs and/or replacements that must be made during the period under consideration. Let $u_{\infty}(t)$ be the expected number of times the component returns to an operating state, assuming that it was operational at t = 0.

It can be shown then that $u_{\infty}(t)$, for large t (steady state operation), is

$$u_{\infty}(t) = \frac{(a+b)mt}{a+b+m}$$

This equation illustrates, then, that in a certain time period T there will be $\frac{(a+b)mT}{(a+b+m)}$ equipment failures of either a false alarm or a no alarm type.

Using this expression, then, the expected number of false alarms in a time period T is

$$E(1) = \frac{amT}{a+b+m}$$

The expected number of no alarms is

$$E(2) = \frac{bmT}{a+b+m}$$

Component testing, though not strictly a parameter of component reliability, is necessary to examine in light of system performance. The purpose of component testing is to maximize the number of components available. There are two distinct cases that must be considered. In the first case, checkout time is not considered as downtime, i.e., the component, even though it is being tested, is available to perform its assigned task; in the second case, checkout time

is considered downtime, i.e., the component cannot perform its assigned task while it is being tested. These two cases will be treated separately. Note that there are really two situations involved in the no-downtime case. The first being situations where continuous monitoring of the component is feasible; and the second, where it is not. Thus there are three cases: (1) no downtime, continuous checkout; (2) no downtime, discrete checkout; and (3) checkout with downtime.

In the first case, where checkout time is not downtime, an optimal checkout period does not exist. With continuous checkout, it can be shown from queuing theory that the average proportion of components, A(0), in repair is

$$A(0) = \frac{a+b}{m}$$

In the second case, again there is no optimum testing interval. If the components are tested at a time interval T_c, then the average number of components out of service is given by

$$A(T_c) = \frac{a+b}{m} + \frac{bT_c}{2}$$

In the third case, however, there is an optimum checkout period given by

$$T_c = \sqrt{\frac{2t_c}{b}}$$

where t_c is the time period required for checkout. The corresponding average component unavailability,

$$A_1(T_c) = \frac{a+b}{m} + \frac{b(T_c-t_c)^2}{2} + \frac{t_c}{T_c}\left(1 - \frac{a}{m}\right).$$

Returning to the original definition of reliability, it should be obvious now that what is really sought is a measure that will give the probability that a given component will perform its function in a warning system when called upon to do so. It must not only be available, say, at time t, but it must not fail in the no alarm state during the warning period t to t + x, where x is the duration of warning. Therefore, a suitable measure of component performance, S, for a single warning is

$$S = [1-A(.)]\ \left[1-\int_t^{t+x} P_2(y)dy\right]$$

Since we are dealing with steady state operation,

$$S = [1-A(.)]\ [1-P_2(\infty)]$$

$$= [1-A(.)]\ \frac{(a+m)}{a+b+m}$$

where A(.) is the appropriate availability function (derived above) and the parenthetical part, (a+m)/(a+b+m), is the probability that the component will not fail off during the warning period of duration x.

5.4 COMBINING COMPONENTS

Since the type of warning systems being considered in this study are of the fan-out variety, this discussion is restricted to the study of a single chain within the fan such that it contains all of the possible components and communication links (which are also components by our definition). By convention, the components are serially numbered from the initiation point (number one) to the terminal point (number "n"). It is also necessary to determine the portion of the population that is served by each component. The initiation point serves the entire population. If there are, say, eight components on the second level, then each of these would serve one-eighth of the population, etc. By convention, the population is defined as the number of terminal points in the system. The probability, S, that the system will properly disseminate a legitimate warning is given by the product of the S_is for each level, or

$$S = \pi_i S_i$$

This value, in reality, is the probability that any randomly selected terminal will receive and disseminate a legitimate warning. This is the first measure of system performance.

The next area to investigate is false alarms. Investigated first is the number of people placed in jeopardy by the failing of the i^{th} component in an on condition; second, the total expected failures of all like components over a given time period; and, last, the average duration of downtime for that component. The last figure does not give the duration of a false alarm, but, rather, gives a time during which a no alarm condition prevails, for a component that fails into an on condition precludes the use of components in the network below that component for warning and thus presents essentially a failed off condition for the duration of repairs to the failed on component. The calculations for the terminals are noted separately in the results because the effect of their multiplicity would tend to dilute the results of computations for the control network.

To determine the average population placed in jeopardy by false alarms at any level, the procedure is as follows: The components are numbered such that the numbers follow the flow of information from the source to the ultimate destination. The point being that a false alarm is transmitted to the population only if those components in the chain below the failing component operate as designed.

Let p_i be the population under the $i^{\underline{th}}$ component; N_i, the number of $i^{\underline{th}}$ components in the system; $E(1)_i$, the expected number of false alarms; and S_j, the ultimate reliability of the $j^{\underline{th}}$ component. Then the population (M_i) placed in jeopardy by the false alarm of the $i^{\underline{th}}$ component is

$$M_i(1) = p_i \prod_j S_j$$

and the average population $M(1)$ placed in jeopardy by a false alarm at any level by any component at that level is

$$M(1) = \frac{\sum_i M_i(1) N_i E(1)_i}{\sum_i N_i E(1)_i}$$

The total number of such occurrences, $\overline{E(1)}$,

$$\overline{E(1)} = \sum_i N_i W(1)_i$$

and the average downtime, $t_d(1)$, is

$$t_d(1) \quad \frac{\sum_i N_i E(1)_i \frac{1}{m_i}}{\overline{E(1)}}$$

Finally, for the no alarm situations, the procedure is as above except that one need not take into consideration system performance below the failed component because the affected population is in jeopardy whether the subordinate system functions properly or not. Thus

$$M_i(2) = p_i$$

$$M(2) = \frac{\sum_i M_i(2) N_i E(2)_i}{\sum_i N_i E(2)}$$

$$\overline{E(2)} = \sum_i N_i E(2)_i$$

and

$$t_d(2) = \frac{\sum_i N_i E(2)_i \frac{1}{m_i}}{\overline{E(2)}}$$

The average downtime, t_d, for any failure is then given by

$$t_d = \frac{t_d(1)\ \overline{E(1)} + t_d(2)\overline{E(2)}}{\overline{E(1)} + \overline{E(2)}}$$

and, of course, the total expected number of failures, $\overline{E}$, is

$$\overline{E} = \overline{E(1)} + \overline{E(2)}$$

and the average affected population, M, is

$$M = \frac{M(1)\overline{E(1)} + M(2)\overline{E(2)}}{\overline{E(1)} + E(2)}$$

The computations and results for the example are contained in Figure 5-11 of the chapter.

Computational forms are also supplied and an example is developed in detail for a five component system.

5.5 DETERMINATION OF REQUIRED COMPONENT RELIABILITY

Frequently, only the desired system reliability is given in system specifications, and it is necessary to allocate required reliabilities (S) among the various components involved. Examples can be found in the 416L (SAGE) requirements which dictated that the system unavailability should not exceed four hours per year, or in the 477L (NUDETS) system which specified a 90 percent availability. In neither case did the reliability requirements go beyond these figures in amplifying the reliability requirements for subsystems or components. System designers cannot, however, trust to luck hoping that the requirement can be met. Therefore, allocation of system reliability requirements is a legitimate area of investigation in this study. Therefore, two cases will be considered: the first being that all components are of equal importance; and the second, that all components are not of equal importance and that their relative importance can be estimated.

Recalling that the probability of the simultaneous occurrence of independent events is the product of the probabilities of their individual occurrences, this fact can be applied to determine the reliabilities of various components connected in series. Thus, if all the components have equal importance, the required reliability of the i^{th} component is

$$S_i = S^{\frac{1}{n}} \tag{18}$$

where

S = required system reliability

S_i = required component reliability, and

n = number of components in the series.

If the relative importance of each component, E_i, has been established, then the problem is to find a number k_i such that

$$\begin{cases} S_i = S^{k_i} \\ k_i = < 1 \\ \Sigma k_i = 1 \end{cases} \tag{18a}$$

After some elaborate manipulation, it can be concluded that

$$k_i = \frac{1}{mE_i} \tag{19}$$

where m is a normalizing factor and is found by the relation

$$m = \frac{1}{n} \Sigma \frac{1}{E_i} \tag{20}$$

Note that the only restrictions on E_i is that it be greater than zero.

In the case where there exist parallel paths, i.e., the configuration is redundant, the duplicate components are lumped together for the initial allocation and are treated as one component. Then, to determine required reliability of each component that has been lumped, one proceeds exactly as above, but instead of using S and S_i in the computations, $Q = 1-S$ is substituted for S, and $Q_i = 1-S_i$ for S_i. This method is applicable only if the system does not require both components for satisfactory operation, i.e., the components in question are truly redundant.

6.0 SUMMARY OF CHAPTER SIX: FEASIBILITY OF USING COMMUNICATIONS SATELLITES FOR PUBLIC ALERTING AND WARNING

This chapter examines the feasibility of using communications satellites for alerting and warning the public in the event of a national disaster. The subject is approached in two ways:

- By determining the capabilities of currently operational or planned communications satellites.
- By evaluating any types of services related to public alerting and warning that may have been planned or proposed.

The study considers two types of operational communications satellites: random orbit and synchronous orbit.

Random-orbit satellites have a limited coverage and require very elaborate and expensive tracking equipment. This means that in order to provide adequate

coverage a great many of them would have to be employed, therefore they cannot be considered feasible from either a technical or an economic standpoint.

The synchronous-orbit satellites can provide adequate coverage with as few as three units, and require no elaborate tracking equipment; however, they do employ rather sophisticated high gain antenna and receiving systems. Thus, they can be considered feasible from a technical standpoint, but the economic aspects of their use is questionable.

From an operational standpoint, neither the random-orbit nor the synchronous-orbit satellites can be considered feasible, because both are highly susceptible to direct attack or jamming.

Recent policy statements issued by organizations concerned with satellite communications (DCA, NASA, and COMSAT) and recent proposals published by RCA and Hughes indicate that some attention is being given to the subject of specially designed satellites to be used for public alerting and warning. However, some of these proposals contain certain state-of-the-art limitations (such as using atomic reactors as power sources) that indicate there is little likelihood that any of these plans would be operational before 1970.

The chapter recommends that no further effort be applied to satellites for either direct public alert and warning or for point-to-point alert and warning relaying from the national level to regional and/or local levels. This conclusion should not preclude further research on the potential of satellites to provide OCD communications, especially in conjunction with the forthcoming DOD military communications satellite system.

Decision-making constitutes a process ending in an act of will of a person or groups of persons who choose between two or more alternatives. Before this final act of will, many other choices are involved--of information sources, of interpretation methods, of values, of objectives, of means, etc. All these additional choices are often made by authorities subordinate to the authority making the final decision, but are at times conclusive in determining the direction of this final decision.

Joseph Frankel, The Making of Foreign Policy: An Analysis of Decision-Making, Oxford University Press, 1963, p. 5.

CHAPTER TWO

DECISION TO WARN

1.0 INTRODUCTION

1.1 SCOPE OF THE STUDY

The warning process consists of many phases, including the entire sequence of actions from threat perception to the decision to warn, to warning dissemination, and finally to completion of the protective reaction. The focus of this study is on the decision to warn at the national level, and as such looks at only the first two phases--the intelligence phase (data input, analysis, and evaluation) and the decision phase.[1]

Throughout this chapter the Cuban crisis of 1962 is used to demonstrate the many facets of the intelligence and decision phases of the warning decision process. This is done for two reasons. First, the crisis was recent and its various aspects are easily recalled. Second, the Cuban situation presented a threat to the continental United States of a magnitude and proximity that has not been equalled in the nuclear age.

1.2 OBJECTIVES

The objectives of this study are to:

1. Review and evaluate the rationale and current procedures that are used to make the decision to alert and warn at the various national locations.

2. Determine the relationships between military and civilian activities that would influence the decision to alert and warn, including any constraints imposed by the international situation.

3. Determine functional responsibilities for the decision to warn, including who would do the warning and when it would be done.

4. Define the information needed to make the decision, and evaluate the capability of current sources to provide such information.

5. Make recommendations, where needed, for changes in the decision-making process.

1. This chapter supersedes The Decision to Warn, which was originally published as TM-L-1960/040/00, dated 6 October 1965.

2.0 CONCLUSIONS AND RECOMMENDATIONS

2.1 CONCLUSIONS

The conclusions that resulted from this study are as follows:

1. Crisis Information. Though only informative and not directive, crisis information can trigger definite public reactions, depending upon how it is presented and interpreted.

2. Absence of Decision-Making Role. The Office of Civil Defense (OCD) does not have a decision-making role in the decision to warn. The OCD role is confined to the input and output stages of the decision process--providing input during the intelligence phase and implementing the warning after the decision has been made.

3. Tactical Warning Decision. The decision to give tactical warning has already been made. OCD doctrine states that if certain predetermined conditions exist, namely that the country is under hostile attack, tactical warning will be declared. This response is effected by the NORAD declaration of an Air Defense Emergency.

4. Strategic Warning Decision. The decision to give strategic warning would be made only by the President. The essential features of a strategic threat are (a) the absence of an identified tactical threat, (b) the volume and complexity of strategic intelligence, and (c) the many possible implications of the decision.

5. Input of Civilian Defense Readiness Information. The role of OCD as the data source and counsel on civilian defense readiness during the intelligence phase of the warning decision process is both logical and appropriate. The agency's performance in this role, however, is greatly encumbered by many organizational and operational problems:

   (a) The data requirements for the decision makers are not explicit.

   (b) OCD does not have a real-time data base and, as such, data response times are slow.

   (c) OCD does not currently have a role in the National Military Command Center (NMCC); prior to the transfer of OCD to the Office of the Secretary of the Army, when OCD did have a role in the NMCC, that role was not sharply defined.

   (d) The interface between OCD and the Office of Emergency Planning (OEP) is not clear.

These encumbrances have resulted in the status of civilian readiness not being fully brought into either tactical action or warning decision-making because OCD does not have the appropriate information to input, nor is it even in a valid position to inform. Except for isolated cases, OCD's resources as an operational organization have not been fully tapped; instead, the agency's role has been relegated to one of planning.

2.2 RECOMMENDATIONS

These recommendations are offered as a means of improving the effectiveness of the national warning decision process.

1. OCD's Advisory Role. OCD's access to data throughout the nation on the civilian defense posture is great, and as such has potential broad flexibility in providing accurate inputs to the decision process. To effect this capability, OCD must maintain continual cognizance of civilian readiness, and must be able to input the data to the decision makers. To accomplish this, the following is recommended:

   (a) Determine what information is needed for the President to make a decision.

   (b) Develop a data base to include the required information, making it not only the source for current information retrieval, but the basis from which projections on future civilian readiness conditions can be made.

   (c) Reestablish and clearly define OCD's role in the NMCC, considering both OCD's contribution to the NMCC and the extent to which OCD can extract information from the NMCC.

   (d) Following reestablishment and definition of OCD's role in the NMCC, designate a sufficient number of OCD personnel, with appropriate security clearances, for participation in the NMCC on a full time basis. This requirement does not exist today, but will be imposed with the implementation of the data base and the definition of OCD's role in the NMCC.

   (e) OCD and OEP must examine their relationship and define and establish a clear interface between the organizations so as to ensure that OEP is aware of the national civilian readiness posture and OCD's capability for changing this posture. This would include the formalization of OCD/OEP information channels.

2. Strategic Direction. Inherent in the decision to warn is the fact that the warning must give direction to do something, and what the people would be told to do would depend upon the level of civilian preparedness. For warning to evoke a maximum, positive response in the minimum time, the level of preparedness would have to be high. Our civilian defense posture, however, is low during normal times, and to bring it up to even a minimum workable level during a crisis would require that the public be given some form of direction.

The basic argument for issuing public strategic warning in a crisis situation is to prepare the nation to survive what is deemed to be an imminent hostile attack. The basic argument against declaring it is that the nation would be formally committing itself to a definite position which, despite the fact that such a commitment would serve to demonstrate the seriousness of the country's intentions, could have the disadvantage of being interpreted as a hostile act which could precipitate preemptive enemy action. A firm national policy in a crisis situation is imperative, but the advantages of being in a state of negotiation for the greatest amount of time without committing the nation to a war footing (a position from which retreat might not be possible) are numerous, particularly if the United States were considering a preemptive attack on a hostile power to neutralize the threat.

Thus, crisis information, though informative and not directive, can trigger definite reactions, depending upon how it is presented and interpreted. A crisis situation in itself sets the mental climate for the interpretation of information. How information might be interpreted in a particular situation can be determined. In a threat situation, then, through the careful management of the timing and release of crisis information, the members of the public could be given a form of direction without having to resort to strategic warning to tell them what to do. This would then allow public strategic warning to be reserved for use as a diplomatic tool in crisis negotiations.

Though it has been suggested that crisis information, not strategic warning, be used as the means to increase the civilian defensive posture in a crisis situation, it is recommended that strategic warning be given to activate the state and local defense organizations. Its use here, preferably before crisis information is issued, would allow the civil defense organizations to mobilize so that they would be in the position to work with the people in bringing their defensive posture up to a protective level.

Some recommended steps in the consideration of this concept as a means of improving the national warning decision process are as follows:

(a) A study should be made on information management.

(b) Long range operations plans should be developed and procedures established for directing increases in civilian defense readiness in a crisis environment. These should be applicable from the federal to the local level. This would include the establishment of communications channels and development of a system for frequent testing. The reliability and security of the communications channels must be ensured, and procedures for the handling of the information when received at the local level must be clearly and carefully established.

(c) Additional communication channels should be established between the federal government and the state governors, and between the state governors and local civil defense organizations.

3.0 THE WARNING DECISION PROCESS

The function of determining whether to warn, how to warn, and when to warn is the warning decision process. The process begins with the receipt of the first identifiable piece of threat information, and continues until the final tactical warning decision is made, or the crisis subsides or is resolved.

The warning decision process separates quite naturally into two phases: (1) the intelligence phase, and (2) the decision phase. The intelligence phase continues throughout the warning decision process, and consists of the analysis and evaluation of threat information in terms of the crisis situation and the country's military and civilian defensive capability to cope with it. The decision phase is also continuous, overlapping the intelligence phase and beginning at that point in the crisis where the possibility or necessity of warning the public is recognized.

The communication of threat intelligence to the public can take two forms: (1) crisis information, and (2) strategic and/or tactical warning.

Crisis information, by its very nature, is informative, not directive. The object of it is to make the public aware of the crisis situation, not to direct them to do anything about it. Crisis information is disseminated either through commercial news facilities or by means of Presidential and other official broadcasts over radio and television.

Warning, on the other hand, is directive. Based upon the threat intelligence, the President may decide to declare a strategic warning. Such a decision would be based upon a deepening crisis situation prior to the detection of an actual attack, and reaction time would probably not be a critical factor. In a strategic warning the President, by means of direct broadcast and/or through official OCD warning media, would tell the public to take some action or actions for their protection.

The decision to give tactical warning is based upon the detection of an actual attack. In this situation, time is of the essence. The North American Air Defense Command (NORAD) evaluates the threat and declares an Air Defense Emergency (ADE). Immediate reaction to the ADE is mandatory if the attack is imminent or in progress; and OCD personnel at the National Warning Center (NWC) respond automatically by implementing the tactical warning.

4.0 CRISIS INFORMATION

In a crisis situation information about the threat is received in many forms. When threat information is analyzed, evaluated, and the facts synthesized into a composite picture, it becomes threat intelligence. If the decision is made to inform the public about the situation, threat intelligence data are released in the form of crisis information. Crisis information, then, is threat intelligence as reflected to the public. It is presented initially to inform the people officially of a critical situation. Continuing crisis information is released to keep the public aware of new developments in the crisis.

Crisis information is disseminated when: (1) the public has been made aware of the threat by unofficial sources and their demand for official information has grown to a point where it is necessary to inform them; (2) public support is needed for a plan to combat the forces creating the crisis; or (3) the public must be informed so that they can prepare to take protective action if strategic or tactical warning appears imminent.

Major crisis information would probably be disseminated by, or in the name of, the President over radio and television and in the press. Continuing crisis information would probably be presented by high administration officials such as the Secretary of Defense, the Secretary of State, or the Presidential Press Secretary. The official nature of an announcement from this level of government tends to attract a wide audience, thus presenting the crisis information to a large percentage of the population.

A prime example of major crisis information presented by a President was the announcement of the Cuban missile crisis in 1962. This action occurred following months of intelligence build-up on increased Soviet military support to Cuba. Dramatic aerial photos of the construction of offensive missile sites on the island crystallized the enemy threat to the United States. When President Kennedy announced the sea blockade, or "quarantine" as he termed it, of Cuba, he presented to the people the first official statement about the crisis.

4.1 DATA INPUT, ANALYSIS, AND EVALUATION

Throughout the intelligence phase of the warning decision process there are successive stages of data gathering, analyzing, evaluating and synthesizing. A large number of intelligence sources routinely gather data concerning enemy threats to national security. These data are sent through established channels to processing agencies, while other intelligence sources acquire data about specific incidents in response to direct requests. In all of these lower stage activities judgements are made as to the significance and reliability of each item of information.

All national threat intelligence categorized as strategic or current intelligence is gathered as threat information and synthesized into threat intelligence by such organizations as:

1. Central Intelligence Agency (CIA)
2. Defense Intelligence Agency
3. State Department
4. National Military Command Center
5. Joint Chiefs of Staff (JCS)
6. Commanders-in-Chief, Unified and Specific Commands

Though by no means all-inclusive, these organizations are representative of the intelligence sources available to the President and his advisors.

In addition to threat intelligence, information on the status of military forces deployed throughout the world is gathered and maintained by many of these same organizations. Both the threat intelligence and the status information are forwarded to the National Security Council through the Department of Defense. It is at the level of the National Security Council that threat intelligence is presented to the President and, in light of the current military posture, recommendations on alternative courses of action are made.

Though threat information is usually subject to careful processing before it enters the Presidential decision stage, isolated reports, particularly of an extremely urgent nature, are sometimes sent directly to the President, bypassing the more formal channels described above. At times, too, the President makes requests for specific information directly to the intelligence agencies.

4.2 EXECUTIVE ANALYSIS AND EVALUATION

4.2.1 The National Security Council (NSC)

The chief function of the National Security Council is to advise the President with respect to the integration of domestic, foreign, and military policies relating to national security. In this capacity, the NSC performs as the President's highest level advisory group in time of national crisis. It is the point where threat intelligence of a military and nonmilitary nature is synthesized to produce recommendations for the most feasible courses of action to combat a threat. These recommendations are presented to the President for his final decision.

4.2.2 Office of Emergency Planning (OEP)

The Office of Emergency Planning is charged with planning for the continuity of the government in an emergency, and with the operation of the National Resources Evaluation Center (NREC). OEP advises the President in coordinating and determining policy for all emergency preparedness activities of government which include:

1. Developing and planning the emergency use of resources, such as manpower, materials, industrial capacity, transportation, and communications.

2. Planning the organization of the government in an emergency, and coordinating preparations for the continuity of federal, state, and local governments.

3. Preparing for the stabilization of the civilian economy in an emergency.

4. Planning for rehabilitation after enemy attack.

The Director of the Office of Emergency Planning is a statutory member of the National Security Council.

Theodore Sorensen, President Kennedy's speech writer and alter ego, has written, "White House decision-making is not a science, but an art. It requires not calculation, but judgement."[1] The judgements, however, are

---

1. Theodore C. Sorensen, Decision-Making In The White House, Columbia University Press, New York, New York, 1963, p. 10.

necessarily made after the President's advisers have apprised him of the evaluated threat intelligence, defense posture, and alternate courses of action to meet the crisis.

4.2.3 Specific Crisis Advisers

Discussed so far have been several agencies involved in advising the President on matters relating to national security. There are, however, examples of Presidents relying heavily on trusted confidants, who were not members of specific organizations designated as Presidential advisory groups. This is particularly true during times of extreme crisis. For example, during the Cuban crisis of 1962, President Kennedy turned to a group of men he designated the National Security Council Executive Committee (ExComm).

"In forming his own personal 'Crisis Cabinet'," it has been observed, "Kennedy moved coldly and decisively. He turned to men he knew and trusted--reaching outside the official bureaucracy of the Cabinet and the National Security Council."[1] A listing of the members of the ExComm illustrates the personalities and talents that focused on this crisis, one that is generally considered the most dangerous threat to confront the United States in recent years:

John F. Kennedy	President
Lyndon B. Johnson	Vice-President
John McCone	Director, CIA
Dean Rusk	Secretary of State
Edwin M. Martin	Assistant Secretary of State, Inter-American Affairs
Robert McNamara	Secretary of Defense
Douglas Dillon	Secretary of the Treasury
Robert Kennedy	Attorney General
General Maxwell Taylor	Chairman, JCS
McGeorge Bundy	Special Assistant to the President, National Security
Theodore Sorensen	Special Council to the President
George Ball	Under Secretary of State
Roswell L. Gilpatrick	Deputy Secretary of Defense
General Marshall S. Carter	Deputy Director, CIA

This group of men guided the course of events through the Cuban crisis, thus utilizing a body of experience that President Kennedy believed was qualified to deal with a specific threat.

---

1. Stewart Alsop and Charles Bartlett, "In Times of Crisis," Saturday Evening Post, 8 December 1962, p. 16.

Crisis situations involve factors transcending the boundaries of traditional organizational responsibilities. Only the Office of the President is capable of focusing these many aspects of a crisis. In the President's assessment, the ExComm, as he constituted it, was able to evaluate available threat intelligence and to advise him in a manner most satisfactory to him and without unnecessary delay.

In more recent times President Johnson formed his own compact group of advisers to deal with current crises. The group is a distilled version of ExComm, sometimes known as "the Big Three" or the "Night Hawks" because of their nocturnal meeting habits as well as daily conferences. The members of this group are men who were also members of the ExComm: Robert S. McNamara, Secretary of Defense; Dean Rusk, Secretary of State; and McGeorge Bundy, of late Special Assistant to the President. Other advisers have been called in on crisis matters[1] as needed.

The Presidential decision is shaped by major forces of influence arbitrarily grouped under three frames of reference: Presidential politics, Presidential advisers, and the Presidential perspective.[2] These frames of reference look beyond the organizational charts into the real, but more nebulous, influences that shape the Presidential decision.

4.3 DEFENSE READINESS

The posture of our military and civilian readiness to meet a given threat will generally influence the timing, content, and method of dissemination of crisis information.

4.3.1 Military Readiness

There are two classic and rather divergent philosophies of defense. One states that we must be prepared to defend ourselves against a threat, but never strike until we have been hit first. The other says that, when threatened, strike first and thus reduce our opponent's ability to hit us. Historically, the United States has always advocated the philosophy of never being the first to attack. This is our stated policy today, and thus we gear our defensive posture to be able to absorb a first strike. For this policy to be successful, an adequate retaliatory force must survive the attack.

---

1. Time Magazine, 30 April 1965 85 (18), pp. 29-30.

2. Sorensen, op. cit., p. 43.

With today's sophistication in nuclear weapons and the means to deliver them to almost any point in the world, we cannot, however, afford to discount a preventive or preemptive attack as our possible reaction to a threat. Many factors, of course, could influence any decision to veer so drastically from our stated policy--whether the threat is to the continental United States itself or a limited crisis situation in some other part of the world; the consequences of such an action; the personality and philosophy of the President and his advisers; and many more. In the final analysis, though, a situation could become critical enough, and the balance of power thrown off to such an extent that preemptive attack might be our only means of defense.

We can expect that any military reaction to a particular crisis will be dictated both by the nature of the threat and the operational readiness, disposition, and logistics of our defensive forces to meet it. This is a prime consideration in the general disposition of our armed forces throughout the world. What would be needed to defend our position in a particular area is determined by the importance the U. S. attaches to the area and the kind of threat that exists or could erupt. For example, the numbers and kinds of men and equipment which the United States maintains to protect our interests in Panama differs considerably from the make-up of our armed forces in West Berlin.

On the other hand, a crisis could erupt in an area where it would not be expected or, at least, where we would not be completely prepared to meet it. In this case a course of action would be chosen based upon the existing defensive posture or, if time and the situation permitted, additional forces could be brought in to allow a different tactical reaction to the threat.

The tactical action decided upon to meet a threat will greatly influence the release of crisis information. For instance, if a crisis occurred, such as a threat to the United States position in a foreign land, and our answer to it would be a show of force to support our intent to stay, then crisis information would probably flow rather freely from the early stages of the crisis. If, on the other hand, a crisis developed which could be met by several alternatives, and the success of any one of them, tactically and diplomatically, depended upon secrecy until the choice was announced or the tactical action taken, then crisis information would undoubtedly be withheld until the appropriate time. Aside from the timing aspects, crisis information might also be tailored in a way to give false information to the enemy and hide our real intentions.

The many factors that govern the release of threat data to the public can be demonstrated quite well by the Cuban crisis of 1962. For months prior to the actual outbreak of the crisis, unofficial information about the Russian military buildup in Cuba reached the people via the various news media. In late August, the first "semiofficial" statement came from Senator Kenneth B. Keating of New York, when he said that he had information that there were 1200 uniformed Soviet troops on the island. The administration's official reply

to all of these reports was that it had no information as to the presence of uniformed Soviet troops in Cuba or of any weapons which could not be considered as defensive. Despite the government's professed ignorance of any potential threat, each unofficial report compounded the public alarm.

On 14 October, the first reconnaissance photos absolutely confirming the presence of offensive missiles in Cuba reached the CIA. On 16 October, President Kennedy assembled for the first time the ExComm to evaluate the situation and decide upon a course of action to meet the threat. After much debate, the alternatives were reduced to two: air strike or blockade. U. S. armed forces around the world were put on alert; the Strategic Air Command and the Air Defense Command secretly began moving to battle stations; and diplomatic forces throughout the world prepared for imminent worsening of the situation. President Kennedy made his decision on 21 October: there was to be a blockade of Cuba. This same day the National Security Council met with the Office of Emergency Planning for the first time to learn of the President's decision. At noon on 22 October, Pierre Salinger, the Presidential News Secretary, announced that the President would make an urgent address to the nation on radio and television at 7:00 p.m.

During all of October the government maintained an extremely tight security cloak on all data about the crisis. There were news reports of increased U. S. air, ground, and sea activity at military locations throughout the Southeastern United States; newspapers printed exclusive "intelligence" reports from Cuban exiles about an offensive build-up on the island; editorial opinions flowed forth in print and over the air; again Senator Keating stated that he had confirmed reports that interm diate-range ballistic missile sites were being constructed in Cuba. To these and other reports the government replied by denying the military alert by saying that the military build-up in the Southeastern United States was "an ordinary thing to do"; and by still professing no knowledge of offensive weapons in Cuba.

When President Kennedy addressed the nation on the night of 22 October, he communicated the first crisis information on the Cuban situation. In hindsight, his statement may have been overdue, for the people were saturated with rumors and unofficial conflicting reports; but had information been released as each event occurred, such as by giving the reconnaissance photographs to the press when they first came in, or by telling the people that the President and the ExComm were debating an air strike as opposed to a blockade, the Russians and Cubans would have had time to alter their tactics which could have negated the effect of our countermeasures, intensified the crisis, or both. On the other hand, to have withheld the crisis information until after the blockade had been effected, President Kennedy might not have gotten the support of the people and the free world in general. Such support was considered vital to the success of the plan. The information had to be withheld until just before the blockade was put into effect to maintain the element of surprise, yet it was necessary to tell the people before it was to begin in order to get public support to carry it out.

Had it appeared that the decision to blockade could not be kept a secret until we were fully prepared to effect it, or had it been decided to try and make the Russians think we were going to do something else, the government might have released tailored crisis information to draw attention to other things. If the President had decided upon an air strike to counter the threat, the content of the crisis information and the timing of its release would probably have been different. The announcement of an air strike could have been made a short time before it was launched to allow the Cubans time to get their people out of danger areas. This humanitarian approach would save more Cuban lives, but it would also allow the enemy time to mobilize its offensive and defensive forces to better meet our attack, and that would cost more American lives. On the other hand, the announcement might have been withheld until after the attack had commenced to ensure surprise, thus permitting maximum strike effect, and minimum loss to our forces. In either case, the need for public support to guarantee the plan's success would not be as vital because if the attack were successful and the missiles destroyed, the threa would no longer be there. There are, of course, many other considerations when contrasting the consequences of so drastic an action as an air strike to those of a blockade, particularly in the area of public reaction, but these are considerations which would affect the choice of the tactical action itself, not when and how the people would be told about it.

4.3.2 Civilian Readiness

Unlike our military defense posture, which is structured to maintain a relatively high level of preparedness at all times, civilian readiness is a varying condition. This is so because civil defense is composed of two aspects, their compatibility being a somewhat fluctuating thing: (1) the program which the federal government provides for survival, and (2) the public awareness of the program, and how prepared the people are to take advantage of it.

In line with our national policy of retaliatory defense, we orient our civilian defense posture toward being able to absorb a first strike. A high percentage of the population must survive the attack, and the nation must remain economically viable for future recovery. To this end the federal government, through the Office of Civil Defense, has spent, and is continuing to spend, millions of dollars to increase the nation's ability to withstand a hostile attack. The National Fallout Shelter Program; the research, establishment, and on-going sophistication of the Attack Warning System; the training of both professional and voluntary civil defense personnel in shelter management, radiological monitoring, and the like; the assistance given industry in the development of emergency operations plans to ensure continuity of management and basic industry survival; these, to name but a few, are parts of the federal government's program for building our civilian defense posture.

The interest in and acceptance of this program by the general public varies depending upon their awareness of the world situation. During normal times when the threat is at a low level, the public attitude toward civil defense is one of relative unconcern, flavored at times with a certain degree of apathy, and even rejection. The people are aware that shelters exist, that they are there to protect them in the event of a nuclear attack; but most of the general public does not know what the shelters will protect them from, or even where their nearest shelter is located. At times a book or a motion picture will appear that will arouse the public emotions to the threat of the nuclear age, but in general any excitement which they cause is short lived and their educational value generally nil because the facts presented are often based upon dramatic, but false, premises.

In a crisis situation the people's concern about the problem grows and declines in relation to the threat itself. The amount of concern that they have, however, is dependent upon the amount of information they receive about the threat, whether official or unofficial, and on how close the threat is to them personally. For instance, the public concern about the Cuban crisis grew with each news bulletin, but it was never as great in Montana as it was in Florida.

In the early stages of a crisis, even before any crisis information is released, the concern is often one of curiosity--people want to know what is happening. As the threat grows and the people learn more about it, this curiosity broadens into wonder, and even worry, about what a person could do to save his life. It is at this point that concern about civil defense readiness begins to increase. The longer a crisis continues, whether it escalates or remains steady, the more concerned the public becomes about preparedness. If the crisis subsides, public concern about civilian readiness levels off and then begins to fade.

In addition to major crisis information, which is specific to the developments in the crisis itself and emanates from the President or other high level government officials, there is what is termed crisis-related information, which is the kind of information people sometimes seek as a result of receiving major crisis information. Though crisis-related information can come from high government levels, it can also emanate from the lower echelons.

Whether the crisis information presented is specific to the threat or only indirectly related to it, it is still only informative, not directive. It can, however, trigger definite reactions, depending upon how it is presented and interpreted. When crisis information is released, some people can be expected immediately to take that information as warning and react in anticipation of a worsening of events. What they do can be foolish, for they are often acting without direction. Others are aware of civil defense or play an active role in it, and these may move into action just to make sure they will be ready in case the threat exceeds the critical point. And there are those who, when officially told about the threat, begin to seek direction on how they can prepare themselves.

Shortly after President Kennedy announced the blockade of Cuba in 1962, a civil defense director of a large metropolitan city was queried by the press on several aspects of civil defense. One of the questions asked concerned the advisability of stockpiling food in the home in the event the crisis escalated. The civil defense director responded by saying that the people should be prepared for any eventuality, and that having extra food on hand would certainly be wise. Based upon this one remark, a rash of food buying spread throughout the city.

Here is a case of reaction based upon misinterpretation. President Kennedy gave specific crisis information in his announcement of the blockade. The civil defense director provided crisis-related information when he spoke on the status of civil defense in his city and the advisability of having extra food in the home. Though to some extent it was the fault of the press for quoting the civil defense director out of context, the people reacted to the civil defense director's remarks as if they were told to do something.

In a threat situation the people should be kept informed so that they may prepare to take protective action if strategic or tactical warning appears imminent. We are handicapped, however, by the fact that the release of crisis information, if not carefully controlled, can trigger unwanted responses due primarily to the varying, but usually low-level, civilian readiness condition. To avoid these potential undesirable reactions, then, what crisis information is released as well as how and where this release is accomplished, will be greatly affected by the existing level of public concern for preparedness as well as the current level of civilian readiness.

In addition to the nature of a crisis and our existing military posture at the time it occurs, our civilian readiness will also influence our choice of a tactical action to meet it. If a threat were such that one reaction to it might trigger enemy action against our cities and population, then certainly our civilian capability to absorb a retaliatory strike would affect the choice of that action over other alternatives which might not have as severe consequences.

4.3.3 Readiness Reporting

Information on the posture of our armed forces throughout the world is reported via the Joint Operational Reporting System (JOPREP). Established by the JCS as a standardized system for the rapid exchange of information, JOPREP was designed to provide the data required by the NMCC, and provides both manual and automatic report processing. Reports are required from the Unified and Specified Commands, the military services, and other defense agencies. The submission of reports is on a periodic or as-required basis after certain conditions are met, such as the declaration of an Air Defense Emergency. Some types of reports cover intelligence of enemy activities, but

the majority of them cover the operational status of our own forces in the continental United States and overseas. Operational readiness, force disposition, logistics, and air lift readiness are the major categories of the reports.

Through the use of this system, information on the defensive readiness of the United States military forces is collected and evaluated at the NMCC. From there it is made available to the National Security Council via the Secretary of Defense.

The role of the Office of Civil Defense in a crisis situation is to advise the President and Secretary of Defense on the state of national civil defense preparedness, and to initiate actions necessary for implementing Presidential decisions. Through the use of his advisory and executive staffs, and with access to state and local government units through the OCD regional offices, the Office of Civil Defense is the logical source of information on organizational and public readiness, and on the feasibility of carrying out crash programs to improve the public defense posture.

A reporting channel for these data had been established through the NMCC. If a crisis reached a given stage, it was intended that OCD participate in the activities of the NMCC. At this level civilian readiness information was to be combined with threat intelligence data for presentation to the National Security Council. Subsequent to the transfer of OCD to the Office of the Secretary of the Army in March of 1964,[1] however, OCD was deprived of access to the NMCC. At the present time readmission of OCD to the NMCC is being negotiated through the Army Staff. Pending readmission, OCD must report defense readiness information through Army channels to the NMCC or through ad hoc channels currently undefined. In addition to the currently non-existent NMCC channel, the Director of the Office of Civil Defense may be asked for information directly by the President, or he may be requested to furnish it directly to other government units, such as the OEP, NSC, or the JCS. He may also be asked to act as liaison between the President and the governors of the individual states.

Additional problems exist, moreover, in the delineation of the kind of data required by the Secretary of the Army, the NMCC, and the President; in the relationships between OCD, NMCC, and OEP; and in the availability of reliable, secure communications channels, especially from federal to state and local levels.

The types of information which might be needed by the President and NSC are not well defined. Since the requirements could be diverse, certain items of information might not be available at OCD headquarters, and the accuracy of

---

1. Department of Defense Directive 5160.50, 31 March 1964.

data expediently obtained in a crisis situation may be low. In addition, the response time required for collecting and organizing the information may be too long for the information to be effective.

The OCD/NMCC channel for furnishing information to NSC and the President is logical and appropriate. Problems exist, however, in its utilization. The tasks assigned to OCD were poorly structured, and the operational interface between OCD and NMCC was not sharply defined. OCD did not normally maintain a position in the NMCC, but participated in it only if a crisis situation deteriorated so as to require a high DEFCON level. The absence of OCD representation in the NMCC in the early stages of a crisis potentially created delay and confusion in the acquisition of civilian readiness information. Also, the extent of this participation had not been formalized. The current renegotiations of OCD's position in the NMCC offers an excellent opportunity for correcting previous deficiencies.

The Director of the Office of Emergency Planning (OEP) is charged with the responsibility of assisting and advising the President in determining policy and establishing responsibilities for all emergency preparedness activities of the government.[1] This responsibility includes coordination of activities and determination of appropriate civil defense roles of federal departments and agencies, state and local organizations, and of private participation.[2]

The accomplishment of these tasks requires an on-going knowledge of the state of civilian preparedness, and OCD furnishes this information to OEP as it is needed. While this channel also seems appropriate, it, too, is not well structured. The division of responsibilities and advisory functions between OCD and OEP is not clear. To a considerable extent these areas of responsibility even overlap.

The Integrated Management Information System (IMIS) will provide OCD with a system for evaluating the readiness of local civil defense programs. This evaluation will add to OCD's store of information available to the decision maker. The system, a subsystem of the IMIS called the Readiness Evaluation System, is designed to provide Readiness Indicators of local civil defense programs, such as community shelter plans, EBS stations, radiological defense monitors, etc., that affect the survivability of a population subjected to fallout.

The Readiness Indicators built into the Readiness Evaluation System are intended to measure a locality's relative potential to survive the effects of fallout and the extent of individual civil defense programs to contribute to this

---

1. Executive Order 11051, 27 September 1962, as amended.

2. Executive Order 10952, 20 July 1961, as amended.

survivability. The Readiness Evaluation System should, therefore, be regarded as indicating the capability of a locality to save lives from a fallout hazard. The CD Local Readiness Report and a summary report, the CD National Readiness Report, will form the basic information on local civil defense readiness for use by the decision makers.[1]

5.0 STRATEGIC WARNING

Strategic Warning is the giving of official direction to the people to take certain precautionary measures to protect themselves in a situation where an enemy attack appears imminent, but has not yet been detected. Crisis information would undoubtedly accompany a warning and continue to be disseminated in the period following the strategic warning announcement. One example of strategic warning might be "stay tuned to your radio for further information concerning the enemy threat." While this is probably the lowest level of strategic warning, it is none-the-less real warning in that the people are actually being directed to do something. An attack has not yet been detected at the time of a strategic warning, so public reaction, while very important, does not have the critical time constraint that is present at the time of a tactical warning.

In all probability strategic warning would be announced by the President. The warning, disseminated over radio, television, and other news media, would have the credibility and wide audience characteristics of special Presidential announcements. His office affords the broadest perspective of a national threat and would be the logical point to make and announce the strategic warning decision.

5.1 FACTORS THAT INFLUENCE THE DECISION TO DISSEMINATE STRATEGIC WARNING

The President would be influenced by a multitude of factors as he arrived at the point of announcing a strategic warning. These factors vary, and their degree of importance will change from crisis to crisis. It is desirable, therefore, to have a firm national strategy to be used as a guide for the allocation of the nation's resources during a crisis.[2]

The President has several sources available to him for developing national strategy. Among these are the Cabinet officers, the National Security Council, the White House Staff, the Department of State, and the Joint Chiefs

---

1. Stanford Research Institute, OCD Readiness - Readiness Indicator - Readiness Model, Draft, 5 February 1965, pp. 3, 4, 20, 21.

2. Patrick W. Powers, A Guide to National Defense, Frederick A. Praeger, Inc., New York, New York, 1964, pp. 33-34.

of Staff. In addition to the executive branch, Congress exercises a key role in the formation of strategy by passing pertinent laws, ratifying treaties, and appropriating funds for the maintenance of the armed forces, important foreign commitments, and government organizations.

An intelligence system provides information relative to national strategy to aid the decision-maker during any specific crisis. Until World War I the intelligence systems of nations were considered primarily as wartime activities. This condition existed in the United States until World War II, after which the major powers continued and increased their intelligence systems in the crisis-laden peacetime era.[1]

In addition to information on the capabilities, vulnerabilities, and intentions of foreign nations, domestic resources and objectives must be known. Civilian and military preparedness would represent large considerations when planning a strategic warning. The percentage of our national budget devoted to civilian and military preparedness indicates, to some degree, the emphasis we place on this phase of our national life as a method of meeting enemy threats to the United States.

Public opinion, both national and foreign, may have considerable influence upon any strategic warning decision. In a crisis environment the news media will play a vital role in shaping the emotional tone of public opinion. The reactions of the public through pressure groups and Congress will be evident to the President, if time is available for these reactions to reach him. Decisions on increased public preparations to meet an enemy threat will demand public support. The President, by virtue of his office, has the ability to shape and direct public support in a crisis environment. Because the issues are generally so complex, the facts so obscure, and the period for decision so short, the American people are usually willing to support any reasonable decision he makes compatible with overall national strategy. This willingness is attested to by the tradition, within the United States, of bipartisanism in dealing with crisis situations.

The ability of the national economy to withstand the expenditure of resources necessary to meet the threat; legal agreements, both international and national; the local political situation; validity of intelligence; qualifications of advisers; and assessment of how far each side is willing to go to further their objectives are but a few of the factors that would influence the strategic warning decision. The President, and his advisers, must consider and weigh all of the factors, but they must also know the limits of their information and the limits of the actions taken. Political campaign plans for the handling of national threats are sometimes dramatic and precise, but once elected the President comes to better appreciate the many limits placed on

---

1. Allen Dulles, New York, The Craft of Intelligence, The New American Library of World Literature, Inc., New York, New York, 1965, pp. 26-27.

his choices of action. He is then acting as the leader of the nation, and in many cases the leader of the free world, as well as the leader of his political party. If he fails to lead, no one leads. "The buck," in President Harry Truman's words, "stops here."[1]

5.1.1 Decision to Withhold Warning

The United States has never employed strategic warning. It would seem, then, that the weight of history is in favor of releasing either crisis information or tactical warning, but not strategic warning. The discovery of offensive missiles in Cuba in 1962 generated crisis information, but strategic warning was not employed. The Japanese attack on Pearl Harbor produced tactical warning to the continental United States after the strike had been completed because it was feared that the Japanese were planning to invade the west coast.

There are foreseeable situations that would dictate a "not to warn" decision in our present crisis-ridden environment. Our government monitors and guides almost all world situations that could erupt into a crisis. It also protects the United States' interests in a crisis situation. To give the public strategic warning would be admitting a loss of control over the situation. This may be the only choice left, but often other alternatives are present which would influence the decision not to give strategic warning:

1. A crisis situation might deteriorate too rapidly for reliable intelligence to be evaluated, and enemy attack preparations might have progressed to a point where tactical warning would be more appropriate than strategic warning.

2. One or two strategic warnings might have been issued with no apparent deepening of the crisis. A public "cry wolf" attitude might have been produced, and it would be felt that another warning would produce no public action.

3. There could be a possibility of giving false warning. The cost of a false alarm to the national economy might be of a magnitude to influence a decision not to disseminate strategic warning.

4. A crisis situation might have progressed to a point where it was apparent that the enemy was prepared to attack. Our plan might be to exercise a preemptive attack to destroy their offensive military capabilities before they could launch their attack. A strategic warning to our population would be withheld to conceal our intentions or the intentions of an ally.

---

1. Sorensen, op. cit., p. 83.

5. A strategic warning to the United States population might be interpreted by the enemy as a hostile act, and this could precipitate a preemptive attack on the United States.

5.1.2 Decision to Warn

It is desirable to protect as many persons as possible in the event that an attack should occur. This rather simple and self-evident statement is, of course, much easier to make than to transform into action. Moving even a portion of a population of one hundred-ninety million into action following a strategic warning would be a formidable task. But if the public had some advance warning of an attack they could, in some situations, take action that would enhance their survivability. To do this they would need protection from fallout. After the attack they would need continuity of government, industry, and service functions to continue some form of living. Strategic warnings might provide enough time for these functional entities to prepare for the attack.

Surprise attack by the major powers seems unlikely during the foreseeable future. The balance of power is such that either side would suffer losses of such enormity that other means of advancing national policy may be more desirable than war. Tactics that use some form or combination of limited strikes, blackmail, manufactured crises, subversion, etc., have been used with varying degrees of success since World War II without the result of a major war. We might, then, expect a continuation of these tactics in preference to a direct attack on the United States either following a strategic build-up or as a surprise.

If this situation existed at the time of a crisis, the President and his advisers might desire to have the enemy know that the United States is serious in its stated policy to initiate some type of deterrent action if an enemy provokes it through threat. A strategic warning to the people of the United States could serve as one factor in demonstrating the seriousness of the government's intentions.

This psychological action against an enemy would, no doubt, be coupled with the desire to prepare population, industry, and local governments for an attack. Undesirable actions on the part of the public might be avoided if advance warning and crisis information were disseminated. Much of the public is unaware or unsure of the location of their nearest fallout shelters, how to prepare shelter in their homes, or how to leave a city if evacuation is desired. Strategic warning might allow civil defense personnel time to guide the public in these matters.

Industry, in order to continue after an attack, must have warning time to shut down in an orderly manner or allow skeleton crews to take their places and continue the industry's function. Some industries can stop operations

immediately, but many others require elaborate preparation to discontinue their operations in a controlled manner. For them, adequate warning time is essential.

5.2 STRATEGIC WARNING DECISION POINT

The strategic warning decision point is the climax of the strategic warning decision process. Up to this point is evaluation; beyond is implementation. It is here that the decision to warn or not to warn is made.

The strategic warning decision point was approached during the 1962 Cuban missile crisis when President Kennedy informed the public of the threat and the action taken to counter it, but stopped short of directing the public into action. Some may argue that strategic warning was implied by the President's announcement, but the fact remains that he did not actually present a course of action that the public should follow to prepare itself for an eventual worsening of the situation. If he had directed the people to take some action, such as, stock additional groceries in their homes, seek out the nearest fallout shelter, or even merely to stay tuned to the radio, the nation would have reached and passed the strategic warning decision point.

6.0 TACTICAL WARNING

Tactical warning is the giving of official direction to the people to take certain precautionary measures to protect themselves as a result of the detection of an actual hostile attack against the continental United States. The attack could follow a period of crisis and strategic build-up, or it could, although unlikely, occur unexpectedly. In either case the detection of the threat, its evaluation, and the dissemination of tactical warning would have to be accurate and swift. The time constraint which exists during the tactical situation, not present during the strategic situation, necessitates formal, predesigned warning procedures and the means to evaluate their effectiveness.

These procedures define the conditions for initiating tactical warning based upon the national strategy of defending ourselves if attacked. Defense of our population, government, industry, and military capabilities depends, in part, upon the amount of warning time the country receives. A vast air defense system has been devised and made operational to provide the greatest warning time possible so that the nation can react positively to the threat. Many contingencies of an attack have been anticipated, and the air defense system has been exercised utilizing the contingency situations. Methods of reacting to a variety of attacks have been devised and the decision to react automatically, in a prescribed manner, have been made. This study, therefore, considers the tactical warning decision, occurring at the time of the attack, as a subprocess, i.e., the implementation of previous decisions.

6.1 INPUT

The federal government, primarily through the Department of Defense, is charged with the responsibility of detecting and recognizing an imminent attack, either before or soon after it has been launched. To accomplish this requires a strong air defense capability with the purpose of saving from destruction as large a percentage as possible of the country's population, government, industry, defensive installations, and offensive forces.

The North American Air defense Command, concurrent with the Continental Air Defense Command, has operational control of the personnel, facilities, and weapons of four component service commands to carry out its mission of the air defense of North America. These commands are:

1. USAF Air Defense Command (ADC)
2. U. S. Army Defense Command (ARADCOM)
3. Naval Forces NORAD Command (NAVFORNORAD)
4. Royal Canadian Air Force - Air Defense Command (RCAF-ADC)

NORAD receives threat information directly from sensor networks in Alaska, Greenland, Canada, Great Britain, the United States, and the Atlantic and Pacific Oceans. These sensors can detect aircraft and other air-breathing vehicles, ballistic missiles over the polar regions of the North American Continent, nuclear detonations in the United States, space objects, and in certain areas, sea-launched ballistic missiles. NORAD headquarters, located in the NORAD Combat Operations Center (COC) at Colorado Springs, Colorado and an alternate operations headquarters (ALCOP) are the central receiving points for this tactical information. Lesser quantities of tactical information of a local nature come to the NORAD COC from NORAD Region and Sector command centers. NORAD interacts with many military and civilian agencies in the performance of its mission and offers the focusing capability for the detection and evaluation of all tactical threats to the continental United States.

6.2 THREAT EVALUATION

The threat detection inputs are received in the NORAD COC. Evaluators in the COC study the inputs, analyze and synthesize the data, and present the evaluation of the threat to the decision-makers for their consideration of appropriate action. Most of the threat detection input systems are complex and their alarms are only circumstantial evidence that an attack is in progress. Evaluators must therefore relate the alarm to other information, such as threat constituting criteria, strategic intelligence, and the general world situation, before forwarding it to the decision makers within the NORAD COC.

One of NORAD's missions is to provide evaluated threat warning intelligence to Canada and the continental United States. NORAD COC gathers data, submits it to a number of tests, synthesizes direct threat with strategic build-up data, and disseminates alarms in the form of DEFCONs and Air Defense Warnings.

There are at least three sources of hypotheses on the way NORAD decides whether or not to declare an Air Defense Emergency or one of the DEFCONs. These are: the statements of NORAD personnel on how this will take place; past behavior of NORAD decision makers during actual crises; and, results of the simulated decision-making exercises conducted at the COC. These three sources only approximate real attack situations. Even considered together they provide only a partial picture of events that might occur. They do, however, point to some general conclusions that will probably be valid for some time.

NORAD has the capability of judging the implications of the data it gathers and evaluates. It knows the system's limitations and its capabilities. There are other decision-making centers, such as SAC Headquarters and the White House, that receive threat information directly from some of NORAD's threat input sources. They may also have some unevaluated data automatically transferred to them through the NORAD COC. However, NORAD is the only entity having direct access to all unevaluated data plus the experienced men and equipment necessary for data evaluation.

6.3 TACTICAL WARNING DECISION POINT

Should an attack occur with little or no warning, an Air Defense Warning Red condition is in effect for NORAD forces. This condition permits the immediate implementation of readiness actions to bring forces to a posture of an Air Defense Emergency pending a formal declaration of Air Defense Emergency by the Commander-in-Chief NORAD (CINCNORAD). Subsequent reversion to lesser readiness conditions and air defense warnings will be effected only by CINCNORAD.[1]

Notice of the Air Defense Emergency (ADE) declaration and a statement of the incident causing the declaration are provided to the Joint Chiefs of Staff via the Air Force Control Point (AFCP). The JCS Telephone Authentication system will be used to authenticate the call. The commander declaring ADE

---

1. Headquarters, North American Air Defense Command; Headquarters, Continental Air Defense Command, Operations, Defense Readiness Conditions, States of Alert, Alert Requirements and Air Defense Warning (u), NORAD/CONAD Regulation 55-3, Secret.

will also stand by to brief an emergency Pentagon conference of the President and the JCS on the telephone when such a conference is convened by the AFCP. A resultant decision by the President and the JCS on the basis of the combined conference may be the declaration of a Defense Emergency. All Commands would then take steps to implement emergency measures on a level with those of NORAD.

Situations other than an attack without warning or a missile attack could precede the declaration of an Air Defense Emergency by CINCNORAD. International relations may have deteriorated to such a degree that measures must be taken to achieve maximum readiness for both military forces and civilian agencies. Significant strategic and/or tactical indications of hostilities against U. S. forces overseas, U. S. allies or possessions, and/or the North American continent may have been received. War would appear imminent. The result could be the declaration of the highest state of preparedness by CINCNORAD for the NORAD forces and civilian agencies whereby all defensive and protective measures are readied for implementation. This declaration is the authority to implement approved military and civilian plans for the defense of the North American continent.

Implementation of the tactical warning decision for the military forces is carried out through the Automatic Attack Warning System (AAWS). The AAWS went into operations on 1 September 1964 as the system used by the NORAD command to warn the military forces in the North American continent of an enemy attack. Nearly 200 sites in the United States, Greenland, and Newfoundland are tied to the network. Plans for extending it to NORAD sites in Canada, in addition to those in Newfoundland, are under consideration by Canadian authorities. If approved, provision of the system in Canada will be a routine installation task.

In addition to its responsibility to warn the military forces, NORAD has additional responsibilities related to the warning of the civilian population.[1] These include:

1. To plan for the participation of OCD in the defense of the contiguous United States and Alaska insofar as air defense warnings are concerned.

2. To display and evaluate the air defense situation in order to determine when and where Air Defense Emergency military air defense warnings are required, and specify the degree of such warnings.

3. To notify the OCD National Warning Center and its alternates whenever there is a change in a Defense Readiness Condition (DEFCON).

---

1. Headquarters North American Air Defense Command, Memorandum of Understanding Concerning the Civilian Attack Warning System Between OCD and NORAD, Regulation 55-23, 30 November 1962, pp. 3-4.

4. To notify the OCD National Warning Center and its alternates whenever an Air Defense Emergency is declared or terminated, and whenever the degree of Air Defense Warning is changed.

6.4 OCD TACTICAL WARNING ACTIVITIES

The Office of Civil Defense is responsible for establishing and maintaining a national warning system for declaring and disseminating warnings to state governments and, by special arrangements, directly to political subdivisions.

NORAD's detection and evaluation system provides the intelligence from which NORAD Commanders determine the probability or imminence of air attack. The tactical information available on the various displays at the NORAD COC includes quantitative estimates of the threat, communications status, and the status of defensive forces. OCD National Warning Center (NWC) personnel have access to all of these data. In addition, they participate in intelligence briefings and have a drop on CINCNORAD's internal tactical phone. In essence, they have the same information available to them as do NORAD threat evaluation personnel.

The NWC personnel use the intelligence information, the military situation, command decisions within the NORAD COC, existing OCD directives, and the status of communications as the basis for carrying out their mission. That mission is to declare the Air Raid Warning and transmit it to the civilian population of the United States.

The dissemination of an Air Raid Warning is accomplished over the National Warning System (NAWAS). The NAWAS is the civilian counterpart of the Automatic Attack Warning System and consists of full-period, private-line voice circuits leased from the communication common carriers.

The OCD NWC is the primary control point for NAWAS. On 1 May 1965 the NAWAS was realigned to create an organization locating the NWC at Headquarters NORAD, Colorado Springs, Colorado; a first alternate warning center at OCD Region 5 headquarters, at Denton, Texas; and a second alternate warning center at the present location of the Washington Warning Area Control Point (WWACP).[1]

---

1. Office of Civil Defense, Realignment, Organization, and Responsibilities of the OCD National Warning System, Memorandum, 13 April 1965, pp. 1-2.

The declaration of an Air Defense Emergency (ADE) by CINCNORAD is the current major criterion for the declaration of an Air Raid Warning.[1] Actions by the military to increase the readiness of their component forces, however, may be performed without the declaration of an ADE on the basis of threat information from BMEWS and other detection sources. BMEWS alarm levels and confidence estimates indicating a missile attack are used by the military to increase the readiness of military organizations. DEFCONS are used by the military and by OCD NWC for alerting OCD Warning Centers, OCD Headquarters, OCD Regions, and the WWACP. Only when OCD National Headquarters deems it advisable or when a high DEFCON level has been reached do the state governments receive official notice of the need for increasing the readiness of their organizations. DEFCON changes are never announced over the NAWAS warning circuit. Such changes are transmitted over the NAWAS control circuit from the NWC direct to the OCD regions and, according to established local procedures, from the regions to the states. Local governments receive notice of the threatening situation from the state governments or from informal sources such as military units.

The decision to warn the public of a tactical threat is made at the national level. In effect, it is a decision that has already been made.[2] The Office of Civil Defense has established standard operating procedures for the declaration and dissemination of Air Raid Warning. Unlike the decision to give strategic warning which would or would not be made by the President during a critical situation, the giving of tactical warning is dependent upon the existence of certain predetermined conditions. Thus, it has already been decided that if these conditions exist, namely, that an attack has been launched against the United States or that the country has been hit by hostile forces, tactical warning will be declared. The role of the OCD Warning Officer at the NWC is not to decide whether to warn or not to warn; rather, it is to implement the foregone decision. Thus, upon the NORAD declaration of an Air Defense Emergency, the OCD Warning Officer immediately and automatically responds by declaring Air Raid Warning.

The greatest effort of the OCD personnel in the tactical warning process is in its final phase, that of implementing the decision to warn. It is here that the problems begin.

---

1. Office of Civil Defense, OCD Warning Center Procedures for Operation of the National Warning System, OCD Manual 4305.1, January 1963, p. 1.

2. As a result of the reassignment of the OCD communication-electronics functions to the U. S. Army Strategic Communications Command (STRATCOM), the responsibility for disseminating civil warning is now formally vested in the hands of a military organization, even though all warning officers are currently civilians.

CHAPTER THREE

LEGISLATIVE AND FISCAL HISTORY OF THE CIVIL DEFENSE WARNING PROGRAM

1.0 INTRODUCTION

This chapter examines the development of the civil defense warning program.[1] It is intended as a resource document for future warning studies. It performs the following functions:

1. Collects material showing the legislative and fiscal history of the civil defense warning program.

2. Analyzes the development of the civil defense warning program. In this analysis emphasis is placed upon the verbal and fiscal interaction of the federal civil defense agencies with various Congressional committees (especially the Independent Offices Subcommittee of the House of Representatives).

3. Details the development of the civil defense warning program. This chapter shows the nature of and requested funding for programs proposed as well as the manner in which these proposals were made; the chapter also shows the nature of and funding provided for programs accepted as well as any identifiable Congressional response to the initial proposals.

2.0 CONCLUSIONS

Funding of the Civil Defense Warning System, with the possible exception of research efforts, has received adequate and consistent Congressional support throughout the program's history.

It is considered that this support can be traced to three basic factors.

1. The original program was an extension of one started by the military and which already had Congressional support.

2. There were no radical changes in program direction from year to year. Rather, the proposals made provided for orderly growth of the system. Thus, Congress was able to judge what was proposed against what had been accomplished.

---

1. This chapter replaces Legislative and Fiscal History of the Civil Defense Warning Program, which was originally published as TM-L-1960/060/00, dated 14 October 1965.

3. About 40 percent of the funds were for the purpose of direct support of the state and local effort.

3.0 GUIDE TO ANNEXES

Annex I to this chapter (pp. 3-12 ff.) covers pertinent excerpts from the hearings on authorizing legislation; Annex II (pp. 3-15 ff.) covers hearings on the status of civil defense; and Annex III (pp. 3-20 ff.) covers hearings on the annual appropriations for civil defense. Annex IV (pp. 3-79 ff.) covers the fiscal history of civil defense warning systems including a summary of total obligations by major warning programs for fiscal years 1951 through 1964; a comparison of selected warning funds requested and those obligated versus the total funds requested and those appropriated; and a year-by-year analysis of funds obligated by the warning program.

4.0 DEVELOPMENT OF THE CIVIL DEFENSE WARNING SYSTEM

Over the years, a number of subsystems of the warning system have been separately justified and funded. In this report, each subsystem is traced from its inception. The subsystems are:

National Warning System (NAWAS)
Control of Electromagnetic Radiation (CONELRAD)
and its replacement,
The Emergency Broadcast System (EBS)
National Emergency Alarm Repeater (NEAR) System
Radio Warning System

Since there have been no specific appropriation limitations on warning, it generally is impossible to show specific Congressional action on funds appropriated for warning versus funds requested. In lieu of this, wherever data were available calculations are made of warning funds obligated as a percent of warning funds requested, and this percent compared to the percent of total funds appropriated versus total funds requested.

4.1 NATIONAL WARNING SYSTEM

Included under this discussion is the system for the transmission of attack warning intelligence from the federal to the state and local levels, and the program for providing financial assistance to the state and local levels for the outdoor warning system.

Work on a national warning system was initiated immediately upon establishment of the Federal Civil Defense Administration in 1950. In the hearings on the authorizing legislation, once certain questions were clarified for the committee members, the program received Congressional support (Annex I. pp. 3-12 f.).

4.1.1 Fiscal Year 1951

For Fiscal Year 1951, $5,758,500 was requested for attack warning and communications, which included $98,000 for operating costs of the warning system, $34,000 for operating costs of the communications division, and $5,626,000 for matching funds for alert and communications equipment.

The civil defense witnesses did not convince the committee that the warning system should be operated by civilian officials. In fact, the Committee report indicated the taking over of this warning function by the civil defense authorities would jeopardize the functions of the Air Force (Annex III, p. 3-22).

The House committee recommended an appropriation of $5,110,000, of which $110,000 was for 100 percent federal contributions to the states, and $5,000,000 for matching state contributions. The Senate recommended an appropriation of $160,000 and $3,840,000 for the same purposes. The actual appropriation included only $110,000 for procurement of communications equipment (including sirens) to be provided to the states on a fully-federally funded basis. No money was appropriated for matching contributions from the states.

4.1.2 Fiscal Year 1952

In the Fiscal Year 1952 estimates, $240,000 was requested for operation of the attack warning system, and $4,200,000 for attack warning system matching funds.

The House and Senate both recommended $240,000 for operations. The House recommended $2,000,000 for matching funds, and the Senate $3,000,000. On the basis of the actual appropriations, $728,167 was obligated under the operations category, and $2,676,230 for matching funds.

This support was apparently due to the fact that the civil defense witnesses were able to explain satisfactorily the difference in responsibilities of the Air Force and the FCDA in the warning area (Annex III, pp. 3-23 f.).

4.1.3 Fiscal Year 1953

For Fiscal Year 1953, the estimates submitted to the Congress provided $590,000 for attack warning operations, and $4,750,000 for matching funds for warning. The House recommended $300,000 and $3,000,000 respectively, for

these purposes. Of a total estimate for operations of $30,000,000 for 1953, $8,000,000, or 27 percent of the request, was appropriated. Of a total estimate of $50,000,000 for matching funds for 1953, $15,000,000, or 30 percent of the request was appropriated. The actual division of funds between warning and communications was not explicitly indicated in the documentation of the OCD budget for Fiscal Year 1953. The actual obligation for matching funds of $969,378 for warning, was approximately 20 percent of the estimate.

There was very little discussion of the warning function in the House hearings (Annex III, pp. 3-25 f.), and none in the Senate hearings. As of the time of the hearings, the warning system covered 174 key points throughout the United States.

4.1.4 Fiscal Year 1954

In Fiscal Year 1954, $1,022,000 was estimated for attack warning operations, and $12,000,000 for matching funds. Of a total of $30,000,000 requested for matching funds, $10,500,000, or 35 percent, was appropriated. Of this latter amount, $3,500,000 was allocated to warning, or approximately 29 percent of the original amount requested. $2,155,487 was actually expended.

The testimony of the civil defense officials in justification of these requests did little to advance the warning cause. Included were such statements to the effect that the warning people were overpaid; that the Committee had acted wisely in the past in reducing the amount of funds requested; and that an increase in warning funds for 1954 was at the instance of the Bureau of the Budget (Annex III, pp. 3-26 ff.).

4.1.5 Fiscal Year 1955

The estimates for Fiscal Year 1955 included $11,000,000 for operations, of which $3,740,000 was for "Operations control services," which included the warning net. $10,025,000 was appropriated. $14,750,000 was requested for matching funds, of which $1,300,000 was for warning. $12,000,000 was appropriated.

The actual obligation for warning matching funds was $1,016,751, very close to the original estimate.

4.1.6 Fiscal Year 1956

In Fiscal Year 1956, $11.6 million was requested for operations, including $4,870,000 for "Operations control services," which included warning. $12,400,000 was requested for matching funds, including $1,000,000 for warning. $2,422,044 was obligated under the operations control services category, and $953,513 for matching funds for warning.

In the House hearings, when questioned as to why the estimate included a decrease in matching funds for warning, the civil defense witness indicated that the program was nearly completed (Annex III, p. 3-32).

4.1.7 Fiscal Year 1957

In Fiscal Year 1957, $17,000,000 was requested and appropriated for matching funds, including $1,500,000 for warning. Actual expenditures for this purpose amounted to $1,193,874.

There was very little questioning on the warning program in either the House or Senate hearings (Annex III, pp. 3-34 f.).

4.1.8 Fiscal Year 1958

During Fiscal Year 1957, FCDA revised its warning system and established what is now known as NAWAS. The total NAWAS estimate for Fiscal Year 1958 was for $1,405,000, with the actual expenditure being $1,073,957.

$20,000,000 was requested for matching funds, including $1,500,000 for warning. $1,615,565 was actually expended for this purpose.

The budget justification indicated that through Fiscal Year 1957, federal contributions of approximately $8,900,000 had been made for warning, and that the state and local governments had spent approximately $11,400,000 additional for this purpose (Annex III, pp. 3-35 ff.).

4.1.9 Fiscal Year 1959

Of a total of $19,400,000 requested for operations in Fiscal Year 1959, $5,262,000 was included for "Warning and operations plans." Information on the details of this item are not available. However, approximately $1,137,000 was obligated for NAWAS and $562,000 for the Washington Area Warning System. No new funds were requested for federal contributions, but $17,000,000 was carried forward from Fiscal Year 1958 for use in 1959. Of this amount, $1,800,000 was for attack warning. $1,571,629 in matching funds was actually expended.

The civil defense witness testifying in the House hearings indicated that the warning net now covered 200 critical points and that they wanted to increase that capability by adding 76 more cities during Fiscal Year 1959 (Annex III, pp, 3-40 ff.).

4.1.10 Fiscal Year 1960

The Fiscal Year 1960 estimates included a request for $28,800,000 for operations, of which $3,502,000 was for warning and communications. $25,000,000 in matching funds was requested, of which $950,000 was for attack warning. The comparable amounts appropriated were $23,285,000 for operations and $10,000,000 for matching funds.

$2,795,937 was reported obligated for warning and communications and $1,087,623 for warning matching funds.

The civil defense witnesses indicated that 276 points were then covered by NAWAS and asked for funds to add 100 more points during Fiscal Year 1960. Changes also were being made to make the system compatible with SAGE (Annex III, pp. 3-44 ff.).

4.1.11 Fiscal Year 1961

For Fiscal Year 1961, $25,750,000 was requested for operations, of which $3,832,000 was included for warning and communications. $24,700,000 was appropriated. $3,873,000 was estimated as being obligated for warning and communications during the year.

$22,000,000 was requested for federal contributions, including $1,455,000 for attack warning. $16,000,000 was appropriated, of which $1,250,135 was obligated for attack warning.

There was very little discussion in the Congressional hearings on the warning problem. The civil defense witnesses indicated they planned to add 70 more points to the warning system during Fiscal Year 1961. (Annex III, pp. 3-46 ff.).

4.1.12 Fiscal Year 1962

For Fiscal Year 1962, $4,382,200 was requested for warning and communications. Approximately $3,400,000 was obligated in 1962 for this purpose. $22,000,000 was requested for federal contributions, including $883,000 for attack warning. $1,527,871 was actually obligated for warning matching funds during the year.

Most of the discussion at the hearings concerned CONELRAD and NEAR. Mention was made of the fact that with the funds requested, the warning system would be extended to the goal of 500 points (Annex III, pp. 3-47 ff.).

4.1.13 Fiscal Year 1963

Funds in the amount of $10,100,000 were requested for "Communication and control," including $1,650,000 for NAWAS and $202,000 for WAWAS. In the budget justification it was indicated that it was expected that the Defense Communications Agency would assume responsibility during the year for NAWAS, operating it on a reimbursable basis. Funds actually obligated by OCD for NAWAS amounted to $424,511.

$665,000 was requested for matching funds for warning. During the year, $1,962,013 was obligated for this purpose.

The House and Senate hearings were concerned almost entirely with NEAR and protection of broadcast systems (Annex III, pp. 3-49 ff.).

4.1.14 Fiscal Year 1964

No estimates were included in the Fiscal Year 1964 civil defense estimates for NAWAS, responsibility having been assumed by DCA. It was indicated that the yearly cost of operating the warning system was $1.7 million, which was now budgeted by the Department of the Army. There was no indication in the hearings as to the amount requested for federal contributions for warning. However, $1,198,123 was obligated for this purpose during the fiscal year (Annex III, pp. 3-55 ff.).

4.1.15 Fiscal Years 1965 and 1966

The hearings for Fiscal Years 1965 and 1966 did not identify any amounts for federal contributions for warning, nor were any obligation figures available at the time of preparation of this report (Annex III, pp. 3-61 ff.).

4.1.16 Summary Fiscal Years 1951-1965

Except for Fiscal Year 1951, when the action of the Congress in denying funds apparently was due to a misunderstanding of the program, the federal warning system and the program to provide matching funds for warning purposes have received excellent financial support from the Congressional committees as compared with the support afforded other programs (Annex IV, p. 3-79).

No questions have been raised as to the necessity for these programs. Dissatisfaction has been expressed a number of times as to coverage afforded by outdoor warning devices, and as to the confusion which has arisen due to the frequent testing of the sirens.

4.2 NATIONAL EMERGENCY ALARM REPEATER (NEAR) SYSTEM

The narrative in justification of the research and development budget for Fiscal Year 1951 included the following:

> 1. . . .
>
> 2. Investigate possible use of the electric power distribution systems for dissemination of public alarms with frequency sensitive devices in homes, office buildings, factories, etc. This contract will be negotiated with Naval Research Laboratory. . . . . $75,000.

The next real mention of the NEAR system was in the hearings on the Fiscal Year 1959 appropriations when discussing the research and development estimate. Chairman Thomas inserted in the record language from civil defense's justifications. There was no discussion on the program (Annex III, p. 3-41).

The program was mentioned by name in the 1960 hearings, but again there was no discussion. $29,840 was actually obligated for the program this year.

$200,000 was requested for NEAR in Fiscal Year 1961, but for other than an excerpt from the justifications, there was no discussion of the program (Annex III, p. 3-47). $87,114 was obligated for NEAR during the year.

The first actual discussion of the NEAR system occurred in the hearings for Fiscal Year 1962 (Annex III, pp. 3-48 f.). $300,000 was requested. Additional funds were obtained in a supplemental bill so that during the year $5,117,792 was obligated. In the hearings conducted in 1961 on the "New Civil Defense Program" by the Committee on Government Operations, Secretary McNamara indicated that the $5.5 million earmarked for NEAR would be "a good start on the installation of a home warning system." He proposed, if the Michigan test of the system proved successful, to begin nationwide installation of the generator equipment expected to cost about $50 million.

In Fiscal Year 1963, $25,000,000 was requested for NEAR. Of the funds appropriated, $3,500,000 was allocated to NEAR, and $3,453,188 obligated.

The justification indicated that at the engineering and technical level, progress in the NEAR system had been satisfactory, and funds were being requested in 1963 for power system surveys ($2,500,000) and for equipment ($22,500,000).

There was extensive discussion of the program in the House hearings (Annex III, pp. 3-49 ff.). Apparently the Committee gained the impression that civil defense was not sure the system would work, and that they did not know how much it would cost if it did work. Mr. Pittman assured the Committee there was no question about it working—the only element of uncertainty being the most practical and effective way to install it in the 3,400 utility companies. Mr. Pittman also indicated he estimated the total federal cost would be $110,000,000.

In Fiscal Year 1964, $4,500,000 was requested for NEAR. It was indicated that the program was still in the engineering development stage and the civil defense witness then indicated a cost of $150 million for the generators.

Chairman Thomas after quite some discussion of the NEAR system (Annex III, pp. 3-51 ff.).

> This is a highly technical matter. I hope you will make it work. When you come in here next year you ought to have this settled one way or another, should you not?

Mr. Pittman replied:

> We are planning on the end of this year as the date when there will be enough data for a decision as to whether to go ahead with the entire system. That will be a few months yet.

In the Fiscal Year 1965 hearings, Congress was informed that no more money would be spent on NEAR, the reason being that "technological developments and the discontinuance of CONELRAD indicate there are other warning systems possible that might be cheaper or more effective." (Annex III, pp. 3- 63 ff.).

The final comment on NEAR came in the Fiscal Year 1966 House hearings when Chairman Thomas asked what had been spent "on the little black box program." It was indicated that $8.5 million had been spent including research costs. (NOTE: The fiscal records indicated an obligation of $9,412,693 (Annex IV, p. 3-83).

The closing comments:

> Mr. Thomas. I wonder why we made that serious error to begin with.
>
> Mr. Durkee. It may not have been a serious error. The reason the NEAR system was developed was because the radio warning system was not available.

4.3 RADIO WARNING SYSTEM

In Fiscal Year 1959, $800,000 was requested in research and development funds for determining the most favorable means of communicating with the people via standard broadcasting stations (Annex III, pp. 3-40 f.).

In the House hearings on the Federal Communications Commission, Chairman Thomas asked the FCC witnesses for their advice on this item. FCC indicated that the proposed system was not very practical. The House did not allow the the funds and in the Senate hearings, the civil defense witness indicated that the cut was not being appealed (Annex III, pp. 3-41 ff.).

During the following years there were occasional questions raised regarding the possibility of using radio as a warning device, but no indication of the feasibility of utilizing such a system was given until the hearings on the 1965 appropriations. The fiscal history indicates that $646,187 was obligated for the radio indoor warning system during Fiscal Year 1964, but there was no discussion on the use of these funds in the 1964 hearings.

In the House hearings for 1965, the civil defense witness indicated that the reason for shelving NEAR was that radio warning systems were now practical. $1.1 million was to be spent in 1965 on the development of such a system (Annex III, pp. 3-63 ff.).

A number of possibilities for utilizing the radio for warning were discussed. The civil defense witness indicated that by the end of Fiscal Year 1965, $1.6 million would have been spent on the final look at the radio warning system.

In the House hearings on the 1966 appropriation, the civil defense witness indicated that technological reports indicated the radio warning system to be feasible, and that they were working with the FCC and radio broadcasting industry on the project. However, no funds for 1966 for this purpose were requested.

4.4 CONTROL OF ELECTROMAGNETIC RADIATION (CONELRAD) AND THE EMERGENCY BROADCAST SYSTEM (EBS)

In the hearings on the authorizing legislation (Annex I, p. 3-13), mention was made of some experiments being made to determine whether or not radio stations could be blacked out to deny their use as homing devices.

These tests proved successful and led to the issuance on December 10, 1951, of Executive Order No. 10312, which provided for the establishment of what was to become known as the CONELRAD program.

From its inception, there was very little Congressional questioning regarding the CONELRAD program or its financial support. The first questions concerning the necessity for such a program were raised in the House hearings on the Fiscal Year 1958 appropriations (Annex III, pp. 3-36 ff.).

In the Fiscal Year 1962, House hearings on appropriations for the Federal Communications Commission, Commissioner Lee indicated that, in his judgment, CONELRAD was the "most important and realistic part of the whole civil defense program" (Annex III, p. 3-47). Late in Fiscal Year 1962, the program for hardening selected broadcast stations was begun. Some 50 stations were so hardened during the year.

In March of 1963, the FCC's National Industry Advisory Committee recommended the Emergency Broadcast System (EBS) to replace CONELRAD.

EBS would permit the stations to broadcast at normal power at normal frequencies. The EBS plan was implemented on August 5, 1963. The impact of this proposed system in the OCD emergency broadcast protection program was substantial in that many stations with low emergency power capability immediately required much greater amounts of emergency power than was needed under CONELRAD.

$6,360,000 was requested in 1963 for hardening radio stations for fallout protection with an estimate of $3,000 to $4,000 per station for fallout protection and $6,000 to $7,000 for auxiliary power (Annex III, pp. 3-53 f.). $1,106,783 was actually obligated for this purpose.

The prepared statement for the Fiscal Year 1964 hearings indicated a plan to provide fallout protection and other emergency features for 192 stations through Fiscal Year 1964. In the testimony for this year, it was indicated that 1369 stations were included in the system. $2,000,000 was requested for 1964 to harden 83 stations and to provide 105 with emergency generators and radio program links (Annex III, pp. 3-55 ff; 3-60 f.). The fiscal records of OCD indicate $3,689,632 was obligated for this purpose in 1964.

In the FCC hearings for Fiscal Year 1965, Chairman Thomas questioned the witness as to why CONELRAD had been abolished (Annex III, pp. 3-61 ff.). The Office of Civil Defense requested $5,579,000 for EBS in 1965. The OCD justification indicated that 191 selected stations had been programmed for fallout protection through 1964 with approximately the same number being equipped with emergency power, radio program links, and associated equipment. During Fiscal Year 1965, an additional 465 were programmed for fallout protection, with an estimated 300 stations requiring emergency generators and 235 radio program links (Annex III, pp. 3-67 ff.). In the Senate hearings for the year, it was indicated that a total of 656 stations were to be provided fallout protection at an average cost of $5,000 (Annex III, p. 3-69 f.). The estimated obligations for this program in 1965 was $3,735,000.

Funds in the amount of $2 million were requested in Fiscal Year 1966 to complete the national coverage requirement of 658 stations.

ANNEX I TO CHAPTER THREE

AUTHORIZING LEGISLATION

Basic Civil Defense Act, Public Law 920, 81st Congress, approved January 12, 1951.

Section 201(c) of the basic act authorizes the Administrator to "make appropriate provision for necessary civil defense communications and for dissemination of warnings of enemy attacks to the civilian population."

In the House hearings on HR 9798, 81st Congress, there were no questions raised regarding the necessity for a warning system as such.

The questioning revolved around three principal items:

1. The distinction between the military's responsibility for gathering intelligence regarding a possible attack, and the passing of this intelligence to civil officials responsible for alerting the public.

2. The necessity for having a separate communications system for warning purposes in lieu of utilizing existing commercial radio capabilities for this purpose.

3. The distinction between a warning system for notifying civil defense officials on a confidential basis of the possibility of attack, and a warning system for notifying the public.

Typical Congressional statements included (p. 7725-7729):

> What effect would a provision like that have on the so-called radar system which the Army is setting up . . . (Mr. Durham)
>
> Now, you would have to avail yourself of all the radio stations in the country and every other means of communication. It wouldn't require setting up an independent system at all. As a matter of fact, if you set up an independent system you would only delay matters . . . (Mr. Elston)
>
> The radar screen is a warning system, is it not? . . . (Mr. Vinson)

> It may not give the news to the public, but it gives the news to certain places and therefore it is a warning system. Under the strict interpretation of this language, you would have jurisdiction of a warning system and, as I interpret it, you would have jurisdiction over the radar screen . . .
> (Mr. Vinson)
>
> My only objection is not to deprive the public of any warning, but it seems to me you have the greatest system in the world already available. Every radio station in the United States would agree that any time you wanted to send out a warning, their facilities would be available. How could you possibly set up a better system than that? . . .
> (Mr. Elston)

Of historical interest, the hearings also included (p. 7226, 7863, 7864, 7866) mention of a study being conducted on utilizing radio for informing the public while still denying an enemy its use as a homing device, later to become the CONELRAD program.

The civil defense witnesses explained satisfactorily the questions of the various Congressmen as evidenced by Mr. Durham's discussion of the program on the floor of the House, included in the Congressional Record of December 20, 1950 (p. 16999, 17000).

Public Law 268, 82nd Congress, March 5, 1952. This act varied the 50 - 50 matching funds provisions for Alaska, and provided authority for state civil defense directors to administer oaths. No mention of warning in the Congressional hearings (S-1244).

Public Law 412, 82nd Congress, June 25, 1952. This act covered leasing of real property. No mention of warning in the Congressional hearings (HR-5990).

Public Law 163, 83rd Congress, July 30, 1953. This act provided for Treasury to assume RFC responsibilities. No mention of warning in the Congressional hearings (HR-5141).

Public Law 383, 83rd Congress, June 3, 1954. This act extended Title III to June 30, 1958. No mention of warning in the Congressional hearings (HR-7308).

Public Law 94, 84th Congress, June 28, 1955. This act covered civilian supergrade positions. No mention of warning in the Congressional hearings (S-67).

Public Law 854, 84th Congress, July 31, 1956. This act adjusted pay for top jobs. No mention of warning in the Congressional hearings (HR-7619).

Public Law 928, 84th Congress, August 2, 1956. This act covered payment of travel expenses for students. No mention of warning in the Congressional hearings (HR-10432).

Public Law 1028, 84th Congress, August 10, 1956. This act covered the acquisition of real property. No discussion of warning in the Congressional hearings (HR-7049).

Public Law 85-606, 85th Congress, August 8, 1959. Although an important law insofar as the direction of the civil defense effort was concerned, the Congressional hearings included few references to warning. Mr. Holifield did mention in the House hearings on HR-7576 (p. 2714): "Clear and prompt warning to the civilian population" as one of the objectives of civil defense. The House hearings also included a brief discussion (p. 2695) as to the difference between warning and communications.

Hearings on HR-3516, 88th Congress, 1st Session.
Part I of the House Hearings includes a prepared statement (p. 3081-3082) on the National Warning System. This statement reiterates the need for warning for people on the fringe of the blast and heat even though "... the fallout shelter program, itself, does not depend on it."

Part I also includes the statement (p. 3115) that "Our own officials admit that Russian civil defense may be better in many respects than that of the United States, although we may lead in warning systems and radiation monitoring."

Part II (Volume 1) of the hearings includes a brief mention (p. 4455) of the problems of warning rural people.

Part II (Volume 2) of the hearings includes a few references to warning, the most pertinent being Dr. Teller's statement (p. 4911): "Shelters are not enough. We need a warning system."

The House Report (No. 715) on this bill (now rewritten as HR-8200) included (p. 33-34) a discussion of warning and communications. Pertinent comments included:

> ... additional warning systems are most important for people outside the area of total destruction but within reach of blast and heat effects.
>
> On August 5 (1963) a new emergency broadcast system was put into effect replacing the CONELRAD system.
>
> The Department of Defense is assisting in modifying selected stations to provide fallout protection and other emergency features. Over 300 key stations are being modified and more will be selected to round out the system.

ANNEX II TO CHAPTER THREE

HEARINGS ON THE STATUS OF CIVIL DEFENSE, 1962

In 1962 the Subcommittee on Military Operations, Committee on Operations, of the House of Representatives, conducted a series of hearings on the civil defense program, with particular emphasis on the national shelter program.

In Assistant Secretary of Defense Pittman's prepared statement, the only mention of warning came when he listed certain conclusions on which the framework of a long-term civil defense program was to be built. One conclusion was "(3) The shelter system should be widely available to provide at least minimum protection to the entire population in places which can be reached on short warning. This requirement makes shelter space in buildings which are lived in and worked in particularly useful (p. 4)."

In a discussion of the civil defense research program, the OCD witness (Walmer E. Strope) used warning as an example in discussing the support systems research program, but there were no questions raised by Congressional members (p. 159-160).

Based on a news story appearing in the papers that day (February 19, 1962), Mr. Pittman was asked (p. 44-45) to comment on the future status of CONELRAD. Other than to say the requirements for restricted broadcasting were being studied, he deferred answering the questions on the basis that the subject had to be coordinated with Canadian officials under a treaty with that country.

Most of the discussion on warning in these hearings concerned two subjects: the National Emergency Alarm Repeater (NEAR) system (p. 172-184), and protection of AM broadcast stations (p. 208-209).

The principal OCD witness (Paul Visher) on NEAR:

1. Explained the necessity for an indoor warning system to supplement the outdoor system;

2. Discussed the alternative systems reviewed for indoor warning;

3. Explained why a system utilizing the electric utility grid networks was decided upon in preference to other systems;

4. Outlined the technical basis on which NEAR operated; and

5. Gave an estimate of $500,000,000 as the cost of a complete NEAR system.

Questions by the Committee members were directed toward:

1. The total cost of the system.

2. Cost of individual receivers.

3. How it was to be financed and managed.

4. Had OCD considered other systems for inside warning.

Total cost of the system (p. 176)

Mr. Riehlman. Then in the last paragraph on page 8 where you refer to this costing about a half-billion dollars, this is just the Government's obligation in being able to transmit this frequency through this gadget or does this include the gadget in the home?

Mr. Visher. The total system cost refers to the combination of the transmitter cost and the cost of all the receivers in the homes. It is estimated this device in the home will cost between $5 and $10 and it is estimated that it will cost between $50 and $60 million to have transmitter-type equipment on a nationwide basis. It is these two figures that approximate the half-billion dollars.

Cost of individual receivers (p. 177)

Mr. Riehlman. I wanted to be sure I understood. What would be the retail cost of this?

Mr. Visher. The cost of manufacture will be between $5 and $10. We are estimating $7 to $7.50.

Financing and management of NEAR (p. 179-182)

Mr. Pittman. May I comment at this point? We may seem a little gun-shy on this question. The background here is that several months ago Mr. Visher started a process of exploring with the utility companies, 3,400 utility systems in the country, what the prospects would be of involving them more deeply than previously anticipated in the management, procurement, and financing of the equipment necessary for this system. In order to really find out what the problems are, it was necessary to put this forward as a tentative plan and ask the utilities, public power utilities and the private power utilities, REA people, all of their associations, to take a close, hard look at something specific. The decision

may have been created at the time that we had made a decision that the financing of both the transmitter and the receivers should be assumed by the utility systems. This impression was not correct at the time and it would not be correct today. ...Now until we are in a position to define the problems more precisely and be sure that the utilities fully understand our problems, we are not taking any positions on the problem of financing, the problem of securing, the problem of management.

.....

Mr. Lankford. You spoke of proceeding on a utility-by-utility basis. You do not mean by that that in some areas it would be managed in one way and in another area managed another way? The whole NEAR system will eventually be managed the same way throughout the country, would it not?

Mr. Pittman. One of the possibilities we are looking at is some variation in methods of managing and financing. This possibility is not ruled out. We can conceive of circumstances in which it would be justified.

.....

Mr. Lankford. Would not the financing have to be uniform throughout the country?

Mr. Pittman. I prefer to keep the question open. Some utilities are in a position to finance the transmitters, there may be reasons why they would prefer to do this. In other cases they would not have the sources of financing available. The Federal Government might then participate in that financing to help out. There may be ways to arrange this. I would like to reserve on this, but we have not closed the door to the possibility of more than one method of financing...

OCD Consideration of other indoor warning systems (p. 177-179)

Mr. Roback. Mr. Visher, this system, would you say, is still in the research and development stage, or is this a system which has now been selected and you are developing or working out the remaining problems in it?

Mr. Visher. I think that it is safe to say that we have selected this system. I think any system—until you finally have all the "bugs" worked out—requires that you always have to keep an open mind on problems which come up. The basic technical feasibility of transmitting a signal has been established. The basic technical feasibility of receiving a signal has been established and I think we should proceed to the system and the implementation of the system as rapidly as possible.

Mr. Roback. Now, you have been the recipient...of proposals for alternate systems...For example, those who are interested...point out that a system which uses radios to give the signal would also convey through this black box information about the warning. It is not going to help the householder very much merely to get a warning noise. He wants to know what the situation is. Now technically, as you have said, there are various possibilities. Are you seriously considering any of these systems or have you signed off on them?

Mr. Visher. I think we are seriously considering any system which proposes different concepts and which we have not looked at previously...It is always conceivable that some new concept might come on the horizon that we had not previously thought about. We are not seriously considering the ones that we have looked at before..... because they are not competitive with the NEAR system from either a cost standpoint or from a reliability standpoint.

.....

Mr. Pittman. May I comment at this point insofar as your questions, Mr. Congressman, goes to our crystallized plans. Our plans are not geared to the possibilities that Mr. Visher has been discussing of what the radio manufacturers might do to take advantage of a going NEAR system. We are not relying on that development. Our plans are confined to the NEAR system outlined by Mr. Visher, as an indoor supplement to the present outdoor warning system.

Mr. Lankford. But you certainly would not rule out any?

Mr. Pittman. Not at all. It would be a bonus if these other developments occurred. But I want to make it clear we are not depending on their occurring.

The OCD witness (Joseph Romm) on the protection of AM Broadcast stations indicated that the Government would:

1. Provide austere fallout protection at transmitters;

2. Provide power generators at the transmitters;

3. Provide radio links between civil defense emergency operating centers and the selected transmitters so that civil defense officials will have a means of broadcasting survival information to the population.

4. Funds expended per station would average $10,000.

The only questions raised on this program concerned the cooperation being received from the stations and from the Federal Communications Commission. Mr. Romm assured the committee that there were no problems from either source.

National Fallout Shelter Program, House Report No. 1754, dated May 31, 1962, by the Committee on Government Operations, was the result of the hearings discussed above. Section IX of the report included the Committee's comments on Communications and Warning (p. 59-65). This report discussed the protection of broadcasting stations; the CONELRAD situation; the role of the Defense Communications Agency in warning; the home warning problem; and the NEAR system.

The information in the report on warning mostly was a repetition of OCD testimony during the hearings. The Committee report did take note of the fact that since the hearings there had been a joint release by the Departments of Defense and State and the Federal Communications Commission announcing a "relaxation" of CONELRAD requirements (April 24, 1962).

The report also took note that the Defense Communications Agency had assumed responsibility for the warning communications net, but that the Office of Civil Defense had retained the actual warning function.

In discussing the home warning problems, the Committee report mentioned three possible systems: telephones, radio, and power lines. It gave quite a lot of attention to the radio system stating: "Proponents of a radio signal system, including radio set manufacturers who see a large new market potential, believe they can overcome cost and reliability objections."

In the NEAR discussion, the Committee explained the present development status, mentioned the total system cost as approaching $600 million, and indicated that the problems of system financing, operation, and maintenance remained to be solved.

ANNEX III TO CHAPTER THREE

APPROPRIATIONS FOR CIVIL DEFENSE

Public Law 45, 82nd Congress, June 2, 1951; and Public Law 253, 82nd Congress, November 1, 1951.

These two acts are discussed together since the first listed covered both Fiscal Years 1951 and 1952.

In the House hearings on the Third Supplemental Appropriation Bill for 1951, the following pertinent comments on warning were included:

> Mr. Cannon. You say that deep shelters are impractical due to the fact that the attack would come without sufficient warning to permit the people to take refuge in them. Your system of communication, then, would be one of the most vital parts of your set-up. What arrangements have you been making as to that phase?
>
> Mr. Wadsworth...The idea is not that we will have no warning but that in a good many cases there may not be sufficient advance warning to fill up a very large shelter where people will have to come from considerable distances and where they would lack the time to get in some large underground shelter.
>
> We are providing a nationwide alerting system which works with the Air Defense Command and we are also providing a communications and message-handling system with a staff in each of the air defense control centers. They will disseminate the warning as given to us by the Air Force. The staff is going to be there 24 hours a day, 7 days a week. That is why we have to have a considerable number of people in this program. (p. 595).
>
> .....
>
> Mr. Taber. It would be more than that. You would not be able to maintain those things without some kind of a set-up.
>
> Mr. Wadsworth. Those people will be in installations owned, equipped, and maintained by the Air Force.
>
> Mr. Taber. By the Air Force?

Mr. Wadsworth. Yes, Sir. The Air Defense Command runs the air-defense control centers, and these people would be the civil-defense part which would disseminate the civil warnings as opposed to the military warnings.

Mr. Wigglesworth. How many people do you have in each of those centers?

Mr. Wadsworth. Fourteen.

Mr. Wigglesworth. Is that a 24-hour operation?

Mr. Wadsworth. Twenty-four hours, seven days a week. (p. 616-617).

.....

The research and development estimate included $100,000 for attack warning, of which $25,000 was for testing of sirens, and $75,000 for investigating possible use of the electric power distribution systems for dissemination of public alarms—the start of NEAR. Committee questions included:

Mr. Taber. What about the attack-warning system?

Mr. Wadsworth. That is the testing of sirens by the National Bureau of Standards to make sure they come up to the specifications we will issue next week.

Mr. Taber. That is within the range of the ordinary fellow's understanding, more or less, and why would such a thing as that cost so much money? It does not sound reasonable.

.....

Mr. Taber. $25,000. Do they not have all of those things like sirens and electric power distribution systems and that sort of thing so that any of those electrical people could tell you just about what they would do without any fussing? (p. 626).

It would appear that the civil defense witnesses convinced the Committee of the necessity for a warning system, but not one operated by civil officials. The Committee report (No. 298, April 6, 1951) stated (page 36):

> The plans upon which the estimates submitted to the committee were based, appeared to be of a nebulous nature and to have been coordinated only slightly with the Military forces of the Nation. For example, funds were requested for an attack warning system to be operated by Civil Defense personnel. At the present time there exists a wholly adequate and efficient civilian attack warning system in the Air Force, and the committee can see no need for the Civil Defense personnel to take over this work. The taking over of this warning system by the Civil Defense authorities would jeopardize the functions of the Air Force.

Page 37 of the committee report included the following statement:

> The estimate received by the Committee for the communication system was $5,660,000. Against this there is recommended an appropriation of $5,110,000 of which $110,000 is for 100 percent federal contributions to the states and the remaining $5,000,000 for matching state contributions.....The Committee has allowed substantially the amount requested for communication equipment which includes sirens, ...It is of the opinion, however, that a more effective and less expensive program can be developed by a greater utilization of existing alerting equipment... For example, the estimate as submitted includes $2,000,000 for the purchase of 2,000 sirens. It would be most desirable to have a special type of siren for all civil defense alerts as is contemplated in the estimates. Certainly, however, there exists in every key center alert signals which can be coordinated with special sirens and utilized in lieu of a complete new system.

Note: The Senate recommended $4,000,000 for the same purposes as above.

In the House hearings on the Supplemental Appropriation Bill for 1952, the following pertinent comments on warning were included:

> Now, as to warning and communications, we naturally say that before civil defense can do much of anything in any of these programs the people on the street must have warning of an attack. It is useless to have shelter unless they have warning and can get into the shelter.

.....

The next chart shows the entire picture of the attack warning system on one page. Over here (indicating) is the Air Force air defense command control center. So far as the Air Force is concerned, their part in this attack warning system stops right here in the air defense control center.

I know that during the presentation last year probably it was our fault that we were not able to convince the committee that we had not planned any duplication of existing Air Force work. We do not have anything to do with the radar or the ground observer corps type of information that comes into the control center, but under Public Law 920 it is our responsibility from that point to disseminate the warning which would finally get down to the services of Civil Defense and, through the sirens, to the man on the street.

.....

Now, attack warning should not be confused with communications. Of course, attack warning depends on communications, but we have split these two programs so that there cannot be any mistake as to what exactly they are supposed to do (p. 650-651).

.....

Mr. Cannon. When this matter was originally taken up and was submitted to the Legislative Committee, the plan was to have this attack warning system handled by civil defense. I believe on further consideration and by the time it was submitted to us for the first appropriation, you decided that that matter could be better handled through cooperation with the Air Force, which would be in a position to handle it without duplication.

In the House hearings on the Supplemental Appropriation Bill for 1952, the following pertinent comments on warning were included:

Now, as to warning and communications, we naturally say that before civil defense can do much of anything in any of these programs the people on the street must have warning of an attack. It is useless to have shelter unless they have warning and can get into the shelter.

.....

Mr. Wadsworth. No, Sir. I am afraid if I gave you that impression we gave you the wrong impression. We never expected to do anything different from what we are now negotiating with the Air Force to do.

.....

Mr. Cannon. As a matter of fact, the original signal as to the coming attack would be handled in their routine by the Air Force and alert signals could be relayed to you without the cost of your maintaining any overall warning system. After it is once relayed to you and received, then you take over on the ground, as I understand it.

Mr. Wadsworth. Under the present plan we would take over in the air defense control center. We would utilize exactly the same means that are now being utilized or would now be utilized by the Air Defense Command to disseminate the information down to the cities where it should go.....(p. 654-655).

.....

Mr. Wadsworth. .....The attack-warning item of $4,200,000 is only for the sirens, their wiring, the control circuits and installation.

.....

Mr. Cannon. You will spend the entire $4,200,000 for sirens?

Mr. Wadsworth. Yes, Sir, for sirens and other warning devices which meet our specifications.

Mr. Cannon. That would aggregate about how many sirens?

Mr. Wadsworth. About 10,988, or nearly 11,000 sirens are represented by this amount.

.....

Mr. Cannon. Would that number be enough to supply every major community in the country?

Mr. Wadsworth. Yes, it would be enough to supply the 69 primary or critical target cities.

Public Law 547, 82nd Congress, July 15, 1952.

In the House hearings on HR-8370 covering funds for Fiscal Year 1953, the prepared statement by the civil defense witness contained the following information relative to warning:

> The attack-warning system can now send an air-raid alert from USAF air defense control centers to 174 key point stations throughout the United States in less than two (2) minutes. (p. 7).
>
> A total of $32,750,000 was allowed by the Congress for six programs in which the Federal Government and the states match funds. For medical supplies, FCDA had $20,000,000; for training and education, $5,000,000; for attack warning, $3,000,000.....(p. 7). (Note: The amounts mentioned covered funds made available in both Fiscal Year 1951 and Fiscal Year 1952).

Other comments in these hearings included the following:

> Mr. Cannon. Now taking up operations, we come to the attack-warning system. Have you been able to make arrangements with the Air Force as to your participation in the attack-warning system?
>
> Mr. Wadsworth. Yes, Sir. We have a written agreement with the Air Defense Command for the placing of personnel in each of the Air Defense control centers, who will be known as attack-warning controllers.....
>
> Mr. Cannon. What arrangement have you made for transfer of funds from the Air Force in that connection?
>
> .....
>
> Mr. Wadsworth. We pay for those ourselves.
>
> Mr. Cannon. You do not get any funds from the Air Force?
>
> Mr. Wadsworth. We will have a transfer of funds from the Air Force for the lease of land lines going from the Air Defense control centers to the key points. They have already made provision, we understand, for that.

Mr. Cannon. In what amount?

Mr. Wadsworth. $600,000, I believe.(p. 23-24)

Although there was no discussion of research funds for warning, a table appearing on page 33 of the hearings listed $25,000 as being allocated for warning and communications research in Fiscal Year 1952, with $100,000 being requested for that purpose in 1953.

The House Report (No. 2316, June 26, 1952) on this bill, recommended the following:

> For operations, $8,000,000, a reduction of $24,000,000 in the budget estimates. Included in the 8 million was $300,000 for the attack warning system (p. 63).
>
> For federal contributions, $29,500,000 of which $3,000,000 was for the attack warning system (p. 64).
>
> Funds requested in the amount of $3,060,000 for research were not allowed in the belief that the major portion of the proposed program represents duplication of work being done by other federal agencies (p. 63).

Public Law 207, 83rd Congress, August 7, 1953.

In the House hearings on HR-6200 covering funds for Fiscal Year 1954, the prepared statement by civil defense included the following:

> Attack Warning.--A major agency responsibility set out in our law and dictated by necessity is to provide early warning of attack to the public, and the civil defense forces of the Nation. It is a military responsibility to operate the early warning net and to collect data of impending attack. It is a civil defense responsibility to transmit that information from the military to the public. The speed and reliability of this warning information must be of the highest caliber. One of our major endeavors is to organize the warning system to permit a greater selectivity between areas. Constant blanket warnings to major portions of the country would stop production and lower morale.
>
> .....
>
> .....In the current fiscal year we will make funds available to the States on a population basis, leaving them the choice of activity--rescue, warden, training, and so on--

so long as they provide an adequate state plan for the utilization of the funds, with priority to attack-warning devices... (p. 224).

Other testimony on warning included:

Mr. Peterson. Project East River was a study... They said, first, we must have increased warning time.

At the present time, the Air Force, whose responsibility it is, says it can give us either no warning time or only 15 to 30 minutes warning of an enemy attack. I think you will see immediately that if we get warning time, 1 to 6 hours of warning time, we eliminate, again, the necessity for these hugh mass shelters because then it would seem to be possible to evacuate our downtown areas. It seems to me that is a sensible approach, provided we can get the warning time . (p. 231)

.....

Mr. Davis. In your attack warning setup, for instance, do you have people there who are paid full time just to stand by for months on end, we will say, or is that organization something that might be compared to the reserves of the armed services, for instance, who are paid only when they are on active duty?

Mr. Peterson. We have only two men who are paid in each one of the--I don't know that I have the right term here--in each one of the air-defense control centers.....

Mr. Davis. He is paid full time?

Mr. Peterson. He is on full-time duty. He is a full-time man and works directly with a full-time Air Force operation. I will say, in my judgement, that we have some overpaid people in those 11 spots. But that is my responsibility as an Administrator, I think, to correct. I have inherited that. I intend to do something about it, if that is what you are driving at. I want to say I am in agreement with you. I haven't corrected it as yet. But I have some people there who are paid about $8,000, or something like that. I think they were recruited originally and set-up on the basis that it required about a colonel to do that job. I will grant you that there is a great deal of doubt in my mind whether it requires the services of a colonel to handle the particular job involved.(p. 240-241)

.....

Mr. Cannon. .....I was gratified to hear you say that in your opinion the committee had acted wisely in the past; that one of the best things that had been done in the review of the budget was to reduce the amount of money asked for this purpose.....As a matter of fact, about the only service your agency could render, Governor Peterson, is first, warning and, second, education.(p. 242)

.....

Mr. Peterson. .....It is true that an attack on Seattle, Washington would probably not be known more than 15 minutes in advance as of today. But thank God because of the geography of our country, if such an attack is made, let us say, St. Louis, Kansas City, or my city of Omaha, are going to get 2 or 3 hours of warning time. It is a simple mathematical problem of dividing the speed of the airplane into the number of miles to be covered. So that parts of America will get a warning.

Mr. Cannon. Do you expect to cooperate with local facilities in your warning system? In any city there are plants equipped with whistles that could be utilized. You wouldn't expect to install any, would you? You would expect to cooperate with those already in existence, commercially?

Mr. Peterson. No, we can't do that. I wish we could. We find it will be necessary to have some distinctive type of warning. It will have to be a distinctive type of horn..... (p. 246).

.....

Mr. Andersen. What, if anything, do you contemplate in planning against the situation that he describes about the evacuation of large urban centers where the traffic would become uncontrollable?

Mr. Peterson. The agency has had the other concept, the concept of going under the ground for the reason that it was not felt there would be any warning time. I can tell you frankly that the military needs the warning time as much as the civilians need the warning time.

Mr. Andersen. Suppose you don't have any warning, and suppose all the roads and highways will be clogged, and undoubtedly they will be as Mr. Cannon has described, because people become panic stricken, do you have any plans to meet such a situation?

Mr. Peterson. Yes, we have the program under which we take over the dissemination of all information in America immediately in the event of an attack. That authority is granted us under the law. We would do that immediately. (p. 248)

.....

Mr. Taber. I notice that you have a breakdown on page 92 of the $14 million. For attack warning there seems to be nearly a $1,500,000 increase.

Mr. Peterson. That is at the instance of the Bureau of the Budget. I think it is based on an appraisal of the situation facing America. It is at their instance that we get an attack warning system completed as fast as possible. We think that it would be 64 percent complete by the end of the year. They insist on 100 percent. If you cannot warn the people then all the money spent by the Air Force on getting the warning to us is of no avail because we are not giving notice to the ultimate consumer. We will try to get that warning finished in 1954. (p. 266)

.....

Mr. Taber. Why do you need all the increase in attack warning?

Mr. Peterson. That is to complete the programs so we can give 100 percent warning to the people involved in the event of an enemy attack and that is the first thing we must have--the warning.

Mr. Taber. How much did you spend on that this year?

Mr. Foulis. $1,876,000 is provided. I cannot answer the question as to how much has been spent so far. (p. 268)

Note: The House Committee recommended $7,900,000 for operations, a reduction of $4,100,000 in the budget estimates. Of the amount recommended, $977,000 was listed for warning. It also recommended a reduction of $20,130,000 in federal contributions to $9,870,000, of which amount $3,300,000 was listed for attack warning (House Report No. 762, July 10, 1953, p. 40, 41).

In the Senate hearings on HR-6200, Mr. Peterson agreed to the reduction in Operations, Attack Warning Program, from the original estimate of $1,022,000 to the House approved figure of $977,000 (p. 139). The Senate hearings also contained the following pertinent comments on the warning problem:

> Mr. Peterson. .....They said three things are required. One was that we must have adequate warning time. At the present time the Air Force, whose responsibility it is to warn the people of America of an impending enemy attack from the skies, says it cannot guarantee that it can give us any warning. If we can get no warning time or even 15 minutes of warning time, there is very little we can do to protect the population other than to train it to duck and take cover wherever it can find it. If that warning period cannot be extended, eventually America will have to face the problem of going underground. It is possible to go underground and to go in far enough to protect yourself against atomic bombs or any other kind of bombs.(p. 149)
>
> .....
>
> Mr. Peterson. .....However, up to this time we have no such assurance by the Air Force. I should point out to the committee that in 10 or 15 years--and I do not know the time, and no one does--it is entirely possible we will have intercontinental, guided missiles that will come across the spaces so rapidly that no detection device, no warning network, will be able to give us any appreciable period of warning. Then we would be back in the same position we are in today. We could have an attack upon the United States without any warning and we would have to take the best kind of cover we could.(p. 150)
>
> .....
>
> Senator Thye. I am somewhat familiar with what existed around the different communities. I have seen it with my own eyes. I just wondered how much it was costing us to conduct that type of program.

> Mr. Peterson. We have spent for the attack warning at the point where I said we step in, $4 1/2 million, Senator. We are asking for $3,300,000 this year to match with the States, and that should complete the program.

.....

Public Law 633, 83rd Congress, August 26, 1954.

At the time of the preparation of this report, copies of the House and Senate hearings on HR-9936, covering appropriations for Fiscal Year 1955, were not available. This report will be supplemented with extracts from those hearings as soon as possible. In the House report (no. 2266, July 16, 1954) on this bill, the Committee recommended (p. 46) $8,525,000 for Operations, which was the same amount as appropriated for Fiscal Year 1954. Direct federal expenditures for the warning net were included under this heading. For federal contributions, the Committee recommended $10,500,000, plus an additional $1,300,000 of previously appropriated funds to be continued available. The new appropriation recommended was the same amount as appropriated for Fiscal Year 1954. In the budget estimates, FCDA indicated an estimated expenditure of $3,300,000 for 1954 for attack warning under this heading, and an estimated expenditure in 1955 for the same purpose of $1,300,000.

Public Law 219, 84th Congress, August 4, 1955.

In Mr. Peterson's prepared statement before the House committee conducting hearings on HR-7278, covering appropriations for the Fiscal Year 1956, the following discussion on warning was included:

> Now I would like to talk about the first phase of civil defense, which is to me more challenging and more intriguing at this time than the second phase. That is the pre-attack phase. What can we do in the pre-attack period to save the lives of our people? The first thing we must have is a detection system which will permit us to know when enemy bombers are on the way to the United States. I am sure you are familiar with the detection systems we are building in conjunction with Canada. When the distant early warning line is completed and we have detection systems extending all the way from Hawaii up to Alaska, Canada, Iceland, and Greenland to the Azores, we hope to have from 4 to 6 hours of warning in the United States. Having that 4 to 6 hours of warning time, it is now our plan to utilize the only tool or weapon that civil defense has in the pre-attack phase, and that is space. That is the only thing we can use today to save lives. The Scandinavians are using space by going underground. They are forced to use it that way because of their location--we can utilize space by moving out of the cities laterally on the face of the earth.

Other questions raised by the committee members were as follows:

Mr. Thomas. Under attack warning, you have set up $1 million for this coming year, a decrease of $1.6 million over last year. Why is that item going down? ... Will you explain why the decrease and what you are going to do with the $1 million requested.

Mr. Peterson. Mr. Chairman, this program covers the placement of sirens in the big cities of America, the target cities of America. May I say that the States and cities undertook this program and spent several million dollars before the federal government ever got into it. In other words, they spent some 11.5 percent of the amount of money covered in the total program before we started. Then we got into it in 1952 and we have been in it ever since. We have now 88.8 percent of this project completed. It is felt that this program has been nearly completed with the exception that there will be recurring costs in the operating of the sirens, and it is felt that we should share in that and contribute toward completion of the system to the extent of $1 million. (p. 409)

.....

Mr. Evins. How much has the Federal Civil Defense Administration spent on warning equipment? Do you have that figure available?

Mr. Foulis. The total amount spent by local and state governments for warning equipment has been $10,569,000.

Mr. Peterson. And we have spent $8,069,000. Some of the large States, like New York, spent a sizeable amount of money before the federal government got into the picture.

Mr. Evins. With the States spending this money, plus the Federal Civil Defense Administration expenditures, would you say that as far as warning equipment is concerned that the program is about completed?

Mr. Peterson. We have about completed it, except probably for devices needed in somewhat smaller cities because of the fallout threat. From now on it will be a matter of keeping it in order. (p. 434)

.....

In the same House hearings (Independent Offices Appropriations for 1956) the Committee also raised some questions with the Federal Communications Commission concerning CONELRAD.

> Mr. Thomas. Mr. Allen, in case of an emergency attack on the country, just what could the Federal Communications Commission do to alert the country almost immediately?
>
> Mr. Allen. The alerting of the country to an enemy attack and the defensive measures, according to my understanding, are the responsibility of the Air Force. They have air defense alarms all over the country. I believe there are some 15 of them. They have the job of alerting not only the military but the populace as well of an enemy attack. Now, in order to implement that, the Air Force has a CONELRAD contract with the Federal Communications Commission and the CONELRAD plan is a system by which the alert from the Air Defense is given; the alert then goes to the various broadcasting stations; it goes to what is called the key stations first, and then it is expanded out from the key stations to the smaller stations. When a radio alert is called after giving the alert--
>
> Mr. Thomas. In other words, every station immediately takes it up, the FM, the TV, and everything else?.....
>
> Mr. Allen. ...After the alert is given to the public, the FM stations and the TV stations go off the air and stay off the air. A certain number of AM stations then go into operation under the CONELRAD plan, in which the stations either go to the 600 or the 1,200 kilocycles.. ...
>
> Mr. Thomas. In case of an emergency, what length of time do you think it would possibly be--after the Air Force announces to the broadcasting system that an attack is imminent--before this information will have been disseminated to every nook and cranny of the United States?
>
> Mr. Allen. The system by which it works, because it is designed to achieve, it is a compromise between the immediate system and the economy of using the present facilities, it has to go through the station, as I said, so that the Air Force directly gives the alert, the radio alert, to the major key stations, they will receive it in a matter of seconds. However, they have to repeat the signal all down the line to other stations, so there may

be a chain of, say, four stations, before it gets to the final smaller station, down in the backwoods somewhere--it may be a matter of a few minutes before they get the signal. (p. 705, 706)

Public Law 623, 84th Congress, June 27, 1956.

Pertinent discussions concerning warning as appearing in the House hearings on HR-9739, Independent Offices Appropriations for 1957, Part 1, are as follows:

Mr. Thomas. .....what does that all mean? "Operations control services."

Governor Peterson. In "Operations control" we maintain the communications system clear across America. That is necessary for us to transfer information from the Air Force in the event of attack upon the United States to the people of America. That means that all of our communications networks, and we have several networks as set forth here in detail, in the material following page 14, all of those networks and all of that material is incorporated in this section and under this division.....

Mr. Thomas. Let me read your own language in there. It is on page 14. Specifically the 1957 appropriation request for "Operations control services" provides equipment and facilities for increased operating capacity through: (1) additions to the existing emergency apparatus staff to provide a nucleus of ready-trained, full-time defense controller personnel; (2) increased communications, including development of methods of indoor warning, improvements of outdoor warning. Can you beat Ma Bell, and the radio and the telegraph and television? Expansion--if you are going to buy all of that--

Governor Peterson. That isn't what we are intending.

Mr. Thomas. We cannot print enough money for it.

Governor Peterson. We are talking here about the siren system. (p. 182)

Mr. Ostertag. The point I am interested in determining is whether or not there is any relationship between civil defense and the Defense Department in the matter of developing a warning and communications system for use in the event of an emergency. Studies have been made and con-

tracts are currently being negotiated. Is there any connection between your responsibilities and the military, and can these responsibilities be coordinated?

Mr. Peterson. Yes. We are very closely related to them, work very closely, and as a matter of fact that closeness of relationship exists not only in the field between our organizations, but also, Congressman Osterta[illegible], exists at the national level. (p. 228)

Public Law 85-69, 85th Congress, June 29, 1957.

In the hearings on HR-6070, included in Part 1 of the House hearings on Independent Offices Appropriations for 1958, Mr. Peterson's prepared statement included the following information on warning:

One of the most critical responsibilities of civil defense is that o. warning the public of impending attack and furnishing information to other federal agencies and state and local civil defense authorities on which they may base their emergency actions.....Consistent with our continuing efforts to strengthen and modernize civil defense, the present nationwide attack-warning system, consisting basically of two major communications networks, is in process of being modified to provide direct nationwide warning from the Continental Air Defense Command (CONAD) Headquarters. The National Warning System (NAWAS), as the modified system is known, will go into operation on May 1 of this year. While it is intended that the initial warning of attack will originate at Continental Air Defense Command Headquarters, should communications into this facility be inoperative at the critical moment, automatic switching equipment will be provided which will permit the FCDA personnel at either the Western or Eastern Air Defense Force Headquarters to take over the warning responsibility immediately.

The modified warning network will permit instantaneous warning of the key points in less than 1 minute. It combines the 2 previously separate networks and places facilities into 1 overall integrated system. Command and control functions can proceed in the same integrated fashion as warning over the 1 combined network, whereas before a distinct break existed between the 2 separate systems. (p. 546)

Other pertinent questions on warning raised in these hearings were as follows:

Mr. Peterson. We have one interesting proposal we are presenting to you today. We believe we will be able by the first of May to cut the warning time down to 1 minute. In other words, in the event of an enemy attack we will be able to warn all of the people in 1 minute. In the past that has taken us as high as 8 or 10 minutes.

Mr. Thomas. I noticed that statement. How effective is CONELRAD and how effective will it be in case you really get into trouble? How are you going to keep people's ears glued to their television or radio? After you once get them to their sets, that is something else.

Mr. Peterson. This is our own internal system under which we will get the warning into each American city. We can do that within a minute from Colorado Springs. With respect to CONELRAD, we just don't know what the future will hold in that area.

Mr. Thomas. From Battle Creek, Michigan, you say you can do that?

Mr. Peterson. From Colorado Springs, where we have liaison people with the Air Force, we will be able to alert state and local civil defense in every city in the United States within 1 minute, should an enemy attack be underway.....

Mr. Thomas. You have to use somebody's facilities?

Mr. Peterson. That is correct.

Mr. Thomas. Suppose they aren't working some place and don't have any radio or television or what-have-you?

Mr. Peterson. You do not understand, Sir--

Mr. Thomas. In other words, you are going to contact every station, and that warning time depends on how many stations are going to have how many listeners?

Mr. Peterson. We are going to contact in the first instance official reception points in every city in America. That doesn't get as far as you are talking about. We can do that in one minute. The next stage will be to get the warning to the people. That is a much more

difficult proposition. This CONELRAD business is one which presently we are considering with the Air Force. CONELRAD was set up because the Air Force wanted to deny the signals of a radio station for homing purposes by enemy airplanes. There are some people who say the enemy isn't concerned with these as a homing device, that they have navigational means--

Mr. Thomas. Isn't that accurate?

Mr. Peterson. I don't know.

Mr. Thomas. They use their own devices getting over here, so they are not going to depend on CONELRAD when they get within 150 miles of the target.

Mr. Peterson. The official Air Force position is that they want to deny this benefit to the enemy. We believe in civil defense that CONELRAD should be eliminated and that we should be permitted to take over all radio and television stations immediately upon receipt of word of enemy attack. We would do this in order that we may constantly broadcast to the people what is going on. We believe that panic and disruption in the country would be caused by lack of immediate information. A man who doesn't know what is going on is a dangerous man. A man who knows what is going on and gets word from official positions in Government is a man who can be relied upon to act somewhat more rationally. That is the theory we are going on.

Mr. Thomas. You are 400 percent correct.

Mr. Peterson. I don't know how that matter is going to be resolved.

Mr. Thomas. Fear is the greatest thing you have to overcome and fear is stimulated and fed by one thing, not having any information. They are lost. If you have somebody to tell them to do this or do that, here is the plan, it takes the edge off. You folks have some pretty good psychologists, haven't you? (p. 551, 552)

.....

Mr. Thomas. Warning and communications, $670,000. What did you spend for it last year? That is pretty good guesswork figure there, $750,000. What did you spend on it last year?

Mr. Starr. Warning communications service will be approximately $750,000.

Mr. Thomas. What do you mean, approximately? You have had only 6 months of this year. How much have you spent in 6 months?

Mr. Starr. We have actually spent about $792,380 so far in the fiscal year.

Mr. Thomas. At that rate, you won't need but $400,000 to be generous about it. You have a tremendous carry-over there.

Mr. Duplantis. There are some items pending--a field test in the internal alarm system that amounts to $600,000. (p. 633).

Mr. Thomas. Warning and communications, $750,000; fire, $250,000; medical, $350,000; human relations, $100,000. We can eliminate all this (p. 637). (Note: the $750,000 discussed above related to funds for research).

In the Senate hearings on HR-6070, the following comments on warning were included:

Senator Magnuson. If something happened right now communication wise, do you take over, or does the military take over with their emergency communications? Or should I put it this way: Or do the two of you get together on it?

Mr. Peterson. We get together. Our men are right there with the military people. It is our responsibility under the law to alert the people of the United States, the civilian population of the United States of an impending attack.

Senator Magnuson. That is wise, because if something happened the military would be busy with their own problems.(p. 227)

.....

Senator Magnuson. It would seem to me that you have a very important role in it and that you have to do some of these things, at least so that the people can be

informed. Now, go back to the communication thing again. I was thinking the American people ought to know. If something happened right now, as you say in most urban centers the sirens would blow and then other things be done according to your plans, but who has the authority? Supposing the sirens blew and somebody got on the phone and told us we should immediately go here or go there or do this or do that? By what authority would he tell us that?

Mr. Peterson. The authority is vested in law. Every state has a civil defense organization and the authority has been vested in that organization by the state legislature. At the federal level it is by act of Congress, Public Law 920. In Washington it would be under the broad supervision of the Congress.

Senator Magnuson. I suppose in lots of cases the orders would come from the local authorities such as the police department, the fire department, and other local people clothed with authority.

Mr. Peterson. Yes, as they share authority from the mayor or from the government through the regularly constituted channels.

.....

Mr. Peterson. In this item there is money in the following fields: Warning and communications research, radiological defense research, fire research, medical research, information and education research, bacteriological and chemical warfare research, and some research in the human relations or psychological field.

Senator Ellender. Are you speaking there for the entire amount you are asking to be restored?

Mr. Peterson. Yes.

Senator Ellender. Would that be $8 million?

Mr. Peterson. $6,700,000 was the total amount we requested, and the House committee gave us $2 million. That $2 million would simply cover the research we want to do in the field of shelter.(p. 237)

Public Law 85-844, 85th Congress, August 28, 1958.

The following excerpts are from Part 2 of the House hearings on the Independent Offices Appropriations for 1959, HR-13856:

Mr. Heffelfinger. We have an item for the Washington area. This is a siren and warning system.

Mr. Thomas. That is for 254 new sirens; when I read that I nearly jumped out of bed. You are not going to have 254 more sirens in the District of Columbia, are you?

Mr. Heffelfinger. Yes.

Mr. Hoegh. That is what it requires.

Mr. Thomas. What do they cost?

Mr. Heffelfinger. They range in cost from $1,500 to $3,500, depending on the size.

Mr. Thomas. Where in the world can you put 250 more? You can hear them 20 miles.

Mr. Heffelfinger. The technicians tell us you cannot hear these sirens in the downtown areas because the buildings absorb the sound. And in the outlying districts there are none.(p. 449)

.....

Mr. Thomas. .....You break this research down to, first, warning and communications, $1,100,000..... You say:

> In Fiscal Year 1959 funds will be utilized as follows: (1) Low-frequency radio communications, $800,000--to determine the most favorable means of communicating with the people via standard broadcasting stations and to determine what use can be made of the system in an emergency.

Are you going to hook up 12 big networks here?

Mr. Hoegh. No, this is different.

Mr. Thomas. What is this? I read that and I could not understand it. What are you going to do here?

Mr. Hoegh. We are going to find out the best means of disseminating information to the people through the use of radio that is now in existence. Tests will be conducted. For instance, there have been some companies that have come up with a project whereby, by a certain lowering of frequency, every man's radio will be turned on full blast and a message would come out.

Mr. Thomas. Regardless of what station his radio was tuned to?

Mr. Hoegh. That is right. That has not been completed.

Mr. Thomas. Whom will you spend this $1,100,000 with?

Mr. Hoegh. There will be several companies. NBC is one of them.

Mr. Thomas. You feed it in one big system and every station gets it regardless of the frequency?

Mr. Hoegh. We are in the process of research in that field.....

Mr. Thomas. You have an item of $25,000 for internal warning systems--

> for analyzer studies of several power systems (connected and independent), to determine typical transmission characteristics and signalling attenuation on different types of powerlines for use in the design of internal warning systems. This would be performed by a contractor that has analyzer facilities. (p. 470, 471)

.....

In the same House hearings, Chairman Thomas asked the Federal Communication witnesses to comment on the $800,000 FCDA has requested for low-frequency radio communications research. Pertinent comments were as follows:

Mr. Thomas. There is one other item about which I would like to ask the help of the Commission, and if you do not mind advising us, we would appreciate it.

One of the items in the budget of the Federal Civil Defense Administration is a low-frequency radio communications item in the amount of $800,000. The reason we come to you people for advice is because you are the experts in this field, and the Federal Civil Defense group is far from being expert, and this committee is even less of an expert.....It does not say how much it will cost to operate it after it is installed. Tell us what you think about it, and what about the overall cost of $10,000,000? Now how much will it cost to operate it after it is put into operation, and how effective is it? Has the Commission considered this idea?

Mr. Lee. Mr. Chairman, this comes within my area as Defense Commissioner. This item has been the subject of discussion by me with our technical people in the Commission.

I should preface this by saying that we have this CONELRAD system with which you are familiar, and we are working out engineering studies to, in effect, extend that system to what we call Phase II. The only reason I mention this background is that it is our feeling, particularly of our technicians, that with these roughly 4,000 broadcast stations around the country--that is, AM and TV stations--we have in effect a built-in radio backup for any civil defense need. Our technical people in the Commission feel that this particular item is not very practical.

The frequency range that they expect to operate in has other users which gives us a problem: somewhat below the radio beacon band. Furthermore, we feel that by the real utilization of all these broadcast facilities at no cost to the Government and just by technical tie-in--that equipment is available--we can provide very adequate backup.

Mr. Thomas. Did you say "at no cost to the Government?"

Mr. Lee. At no cost to the Government; yes, Sir.

Mr. Thomas. How much would it cost to operate it after you installed it at a cost of $10 million or $12 million?

Mr. Lee. I would not be expert on that. I would like to have Mr. Allen, our Chief Engineer, comment on it.

Mr. Thomas. What about it Mr. Allen?

Mr. Allen. I would like to say that we are having discussions with civil defense at this point, and we hope that our technicians can point out to them the advisability and the advantages of utilizing what is already here without any cost. You understand that this CONELRAD system now is for all practical purposes so far as the broadcaster is concerned, without cost to the Government. There are certain costs borne by the Air Force.

Mr. Thomas. And it covers the country like a blanket?

Mr. Allen. That is right; you have everything. (p. 703-705)

.....

There followed a discussion of the estimated yearly operating costs of the system once it was installed. After a lot of guessing, the FCC witnesses agreed that $1,000,000 a year would be a reasonable figure for operating costs for 10 stations. The questioning continued:

Mr. Vursell. Would there be any benefit in this new proposed tieup with the civil defense with reference to timing of an attack? In other words, if you folks can go in and if the radio people could go in and if they have the information, there would not be anyone else on the air with any radio station in the Nation except broadcasting what was about to happen; is that right? That would be from the grassroots up—in TV, and everything else?

Mr. Hyde. One of the great advantages of using broadcast stations--and this has been recognized in the CONELRAD program--is that they already have the ears of the public. They turn to the broadcast station for emergency information.

Mr. Allen. My understanding is that this low frequency network which is being proposed here is a backup network. In other words, it would carry the programs to the various broadcast stations. So, the public would still listen to the regular broadcast stations, and this network would back up in case of line wire failure, and things of that nature, to tie the various broadcast stations together. It would also be an information network by which the Civil Defense Agency would communicate from one point to another in case of the failure. It would not broadcast directly to the public. You would have to have special receivers to get this broadcast. The talks between us and the FCDA

> staff are still at a very preliminary stage, but I think that we probably can work this thing out within the network of the CONELRAD system. I think we can make a very satisfactory solution.
>
> Mr. Vursell. I am in hopes you can, because I thought at the time that this would be quite expensive and probably not too necessary. (p. 706)

.....

In the Senate hearings on HR-11574, the following statement appears in the prepared statement of the Administrator, FCDA:

> FCDA does not wish to appeal the $800,000 for low frequency receivers mentioned in the House report. FCDA has been concerned for some time with the slowness of getting attack information to the public. A number of studies have been made in an effort to determine the best feasible way of disseminating such information. Studies by Melpar, Inc., the Rockefeller Foundation, the National Broadcasting Co., and Gautney Jones (sic)[1] have convinced us that the system presented in the 1959 budget is the most effective solution to this probelm. This has been confirmed by such eminent people as Brig. Gen. David Sarnoff, chairman of the board, Radio Corporation of America, and other well-known experts in the field. In the testimony of the Federal Communications Commission before the House Sub-committee on Appropriations, the Commission was of the opinion that the so-called Phase II system of CONELRAD was more feasible. FCDA is quite familiar with the Phase II CONELRAD system and feels that it is not adequate. However, in recognition of the competence and experience of the Federal Communications Commission and in the best interest of the taxpayer, the request for these funds is being deferred pending further study. (p. 196)

Public Law 86-255, 86th Congress, September 14, 1959

In his opening statement before the House committee which conducted hearings on the Independent Offices Appropriations for 1960 (Part 2), Mr. Hoegh said:

> Our warning capability has been materially improved. You provided funds to increase the number of strategic points that would receive simultaneous warning. We now have 276

---

1. Gautney and Jones.

> key points in the Nation that can receive warning within 15 seconds after the attack is detected. In addition, we expect to have 88 radio stations and 12 tie-ins to radio networks by July 1, 1959, and we are asking you to permit us in Fiscal Year 1960 to extend this warning net to 100 additional points throughout the country. (p. 340)

The House hearings for the year included a number of inserts from the OCDM budget concerning warning (p. 332, 334, 335, 338, 339, 423, 424, 425, and 468). There was very little discussion on the substance of the warning system. An explanation of how the system worked is covered on pages 426 and 427. The research and development part of the budget for Fiscal Year 1960 provided no funds for warning (p. 511).

In the Senate hearings of HR-7040, the following discussions on warning took place:

> Mr. Hoegh. Yes, Sir. This is what we would like to do, Mr. Chairman. First, we want to extend our warning system to an additional 100 target cities in the country.....In addition, I must have six additional personnel to man our warning system at the 30th SAGE Air Division, which is being established by the military this year, so that we can give the warning from that point as well as the other four points.
>
> .....
>
> Mr. Hoegh. No, $165,000 for the warning net, to the additional 100 points and about $46,000 for the personnel to man the 30th SAGE Air Division.
>
> Senator Magnuson. All right. Unless about $211,000 of the $5,515,000 is put back, your testimony is you cannot extend the warning to these other cities; is that correct?
>
> Mr. Hoegh. They would be in jeopardy; yes, Sir.(p. 69, 70)
>
> .....

A discussion of the meaning of warning signals (p. 71, 72) included the following:

> Senator Magnuson. How is it determined as to when they are to blow them? Is that done locally?
>
> Mr. Hoegh. Yes, Sir.

Senator Magnuson. They are blowing them all the time out in Seattle, and if they really need to be blown at some time in the future I do not think anybody is going to pay any attention to them because you know the old Navy story, "No fooling, this time, because there is a fire in the galley."

Mr. Hoegh. Well, I think this policy we have established is right. We give the warning to the local community. We say "Have a competent staff there to analyze the information we give you; if we give you a warning time, and say it is estimated that the planes would not hit Seattle until 2 hours and 12 minutes," then his staff should be capable of advising the mayor and he has the responsibility to make the decision. Either he tells his people, through the warning signal, "Take cover" or "Move out", but it is his decision. Therefore, he must have a good staff, so that he will make the right decision.

Senator Magnuson. In most cities now, you must admit when they blow them, nobody pays any attention to them.

Mr. Hoegh. We do have this situation, Senator.

Senator Magnuson. Well, they just keep on going about what they are doing. How are they going to know whether one is the real one?

Mr. Hoegh. Before I was in the civil defense I was in Chicago one day when they had an Operation Alert. I heard them. I opened the window so I could hear them better. You know I stood there and I thought, "Now, what am I supposed to do?" This makes you realize that you should become informed. Now, I hope that cities only blow these sirens sufficiently enough to create a seriousness in the minds of every citizen so that he will resolve to do something about preparing himself for sustaining himself.

Senator Magnuson. I think that is the weakness of the whole civil defense program, that too many people do not know what to do even if there was a real one. (p. 71, 72)

Public Law 86-626, 86th Congress, July 12, 1960.

The House hearings on HR-11776, covering appropriations for Fiscal Year, 1961, included the following information on warning in the opening statement of Mr. Hoegh:

> Our national warning system can alert today approximately 300 key points in less than a minute. You will recall last year we had 276 such points, and by July 1, 1960, we will have 376 such points. You provided the funds to enable us to do this. In Fiscal Year 1961 we are requesting extension to 70 additional points. Therefore, at the end of Fiscal Year 1961 we would have 446 critical points which would receive simultaneous warning of an attack within a fraction of a minute. As you know, our personnel sit with NORAD and the SAGE divisions, and they have access to the same information as soon as an attack is detected. They then can pick up the telephone line and inform 446 critical points simultaneously of the impending attack.(p. 1072)

Again, there was very little discussion of the warning problem. An excerpt from the budget document on warning is included on page 1089. This excerpt included the information that the NEAR system, for which $200,000 was requested for initial installation, was the first major breakthrough in the field of improved warning capability.

Independent Offices Appropriations for 1962

Part 1 of the House hearings on the Federal Communications Commission included the following on CONELRAD:

> Mr. Thomas. What bearing does this have on our CONELRAD system?
>
> Mr. Lee. It is intertwined, of course. The CONELRAD program, in my judgment, is probably the most important and realistic part of the whole civil defense program. It is something that you can really demonstrate in an emergency.
>
> Mr. Thomas. What is CONELRAD? Explain it again for the record.
>
> Mr. Lee. The term means the control of electromagnetic radiation. The word "conelrad" is a contraction of that term.
>
> This was a requirement that was set down after the Korean war when the Air Force determined that for purposes of navigational aid in time of emergency, they did not want any radiation from any source because this would be a guidance to enemy aircraft.

At the same time, the then Civil Defense Administration indicated that this was the very time when they needed avenues of communication to the people, and it would be terrible to close them down. So then President Truman sent an Executive Order to the FCC as the expert body in this field, and asked us to devise a plan that would meet these entirely divergent needs of these two agencies. Our boys came up with this highly detailed and complicated system of controlling radiation. Under the plan we permit broadcasts on two frequencies, 640 and 1240, for short periods of time.

And what it amounted to was a kind of compromise on the part of both the military and the civil defense people. It was agreed that there was a degree of calculated risk for the requirements of both services, but it was the best that could be worked out. And it is working, I believe, very well.....(p. 699).

Mr. Lee. .....Of course, we would have to continually operate the CONELRAD system, depending on the duration of the emergency. We have detailed plans not only at the national level as to how you get the President on the air and get Government information out, but we have industry committees in each of the 50 states now that are working with their Governors and with the local people to find a maximum of utility for the communications system (p. 700).

Part 2 of these hearings covered appropriations for the Office of Civil and Defense Mobilization. Excerpts of the testimony on warning follow:

Mr. Boland. What are our different warning systems, and how many are there and what do they do?

Mr. Ellis. For the new system that we are now requesting, the NEAR system, and for which we are undertaking a complete pilot survey in the State of Michigan, we are asking for $300,000 additional funds. It is a program which seeks to amplify and to supplement the warning system--carrier system--by filling the gaps that exist in the siren warning setup, by developing the utilization of generators and power and the education of people to purchasing small devices which would be located in each home. Someday I hope every State in the Union and individual citizen will have them.

Mr. Boland. But as a system, it is just coming into being this year?

Mr. Ellis. We have tested it laboratory wise and know that it will work and we do know it is an outstanding communications system. (p. 660, 661)

.....

Mr. Berry. Yes, Sir. It is a recurring cost, except for additions to the system in the year and, of course, the addition to the system involved in this appropriation is an additional 53 warning points. Each year there has been money in it for increasing the number of warning points and, of course, for the recurring cost of the system itself. The 53 warning points involved in this appropriation will bring us up to our goal of 500 warning points that we have felt were necessary (p. 663)

Independent Offices Appropriations for 1963

Part 3 of the House hearings includes, on pages 89 and 90, information from the budget justifications concerning Warning and Alert. The entire amount requested, $25,000,000, was to be spent on NEAR, $2,500,000 for power system surveys, the balance on generators, coupling and synchronization equipment for installation in selected systems. The civil defense witnesses were questioned at some length about this system (p. 90 through 97). Pertinent extracts from the testimony follow:

Mr. Thomas. Now we have national emergency alarm repeater. What is to be the total and final cost? We have $25 million here but what will be the ultimate cost? Some people came up with a figure of $500 million and others have said $1 billion. We have $10 million in 1962, $25 million this year. I notice here you have several months delay for 1962. If you have this delay for 1962, how many months delay will you have for 1963, Mr. Pittman?

Mr. Pittman. Once the delay is over we are going to move very rapidly. The reason for this delay is a technical problem which I will have Mr. Visher explain to you. It concerns a new development by appliance manufacturers.

Mr. Visher explained the problem of operating frequencies.

Mr. Thomas. For this reason your equipment is being modified to operate on a higher frequency to avoid this potential conflict?

Mr. Visher. That is right.

Mr. Thomas. How much time will it take? When will you get in business?

Mr. Visher. We are working with about three utilities at the present time. We expect to have test hardware of a new configured transmitter in the next 3 1/2 or 4 months.

.....

Mr. Thomas. How does this system differ from the old one? What is the need for a new one? Tell us about NEAR. What is wrong with the old system? How much is this going to cost you over the next 5 years? Is that figure of $500 million right that we heard some time ago?

Mr. Visher. The figure of $500 million appears to be the best estimate yet. That is for a total program cost including receivers and transmitters.

.....

Mr. Ostertag. It states in your justification that the total NEAR system is expected to cost in excess of $600 million.

Mr. Visher. This is part of the change resulting from a change in transmitter. The transmitter costs appear to go up slightly, but the recently estimated drop in receiver costs brings the total down since preparation of the justification.

Mr. Thomas. Why the change now? Let us get to the chronology. You have had a system in effect for 10 years. Why the change? What efficiency will the NEAR system have over what you have now?.....Explain what we have had for the last 10 years and then tell us what you are doing by the change that will cost from half a billion to a billion dollars.

Mr. Visher explained the outdoor warning system and the necessity for an indoor system which NEAR was to cover.

Mr. Thomas. Do we know NEAR is going to work yet? Do we have that specific proof?

Mr. Visher. We have specific proof you can transmit these frequencies over long distances and that you can receive frequencies of----

Mr. Thomas. Will this new system eliminate the need for your entire alarm system that you have had for the last 10 years?

Mr. Visher. We do not believe it will. We believe there is still a need for an outdoor warning system.

Mr. Thomas That will not be changed?

Mr. Visher. People in cars, people outside, will receive no benefit from the NEAR indoor warning.

Mr. Thomas. Start at the beginning. How does your present warning system work?

Mr. Romm explained the existing warning system which then terminated in 450 points, to be expanded to 500 points that year.

Mr. Thomas. How does this NEAR system change all that?

Mr. Visher. The NEAR system changes this by taking it automatically from the point of decision to warn the public down through these wires and is automatic, without going through a human evaluation and automatically triggers a transmitted----

Mr. Thomas. It still goes to the seven command headquarters, doesn't it?

Mr. Visher. Yes; and it goes down from there. It can go from the point of decision to warn the civilian population.

Mr. Thomas. Does it still have to go to our state and regional headquarters?

Mr. Romm. You go down through parallel channels. This means it can go down through the utilities grids to make the decision to alert the civilian population. This activates a transmitter which is on the utility grids and this signal goes out. It can also go down through the NAWAS net to go into the local utility grids. There are some 3,400 utility networks we have to tie together.

Mr. Thomas. This will cost from $500 million $1 billion. How much more accurate will it be than what you have now?

Mr. Pittman. There are two main changes. One is to bring the warning into the homes where it is necessary, we believe, for an effective warning system. The other is that the system would work faster. It will be a more instantaneous warning. To make effective use of any system of shelters, we think both a greater reach of the warning system and greater speed could result in a direct saving of many lives and we think it is worth it.

There followed a discussion of the cost of NEAR and the method of financing it. Mr. Pittman indicated that the ultimate cost to the country would be around $600 million but that a decision on how to finance this cost had not been reached. The committee's questions were directed toward trying to find out how much of this amount would be federally appropriated.

Mr. Thomas. From what you see of the program, is it worth the money to start this new program which could easily cost the taxpayer $500 million. That is the question I want to have answered.

Mr. Pittman. The answer is clearly "yes," in our view. In the alternative plans I have described here, neither one would cost the taxpayer anything like $500 million, the total cost figure which we estimated, because the cost of the units to go into the home would not be borne by the Federal Government.

Mr. Thomas. Can you improve on the system that you already have and that you have bought and paid for?

Mr. Pittman. We think it should be many times more effective. We have serious reservations about the effectiveness of the present system.

.....

Mr. Thomas. Well, in either case, regardless of how they are warned, they will be going to the same location and it is a question of which is the more effective warning. Now, a warning system is quite valuable. There is no question about this, but you apparently do not know whether this system will work regardless of its cost.

Mr. Pittman. There is no question about working. The only element of uncertainty is, which is the most practical and effective way to install it in these 3,400 utility companies.

.....

Mr. Thomas. How long will it take you to complete the job?

Mr. Visher. It will take about 2 years to install the system in a total sense once all the operating details--

Mr. Thomas. One year's leadtime in procurement of the items, and another year installation time?

.....

Mr. Visher. I think it will take a year starting from July of 1962 to July 1963 to spend this first one-fourth of the program, and the following three-fourths will start July 1963.

Mr. Thomas. How long will it take you to install it?

Mr. Visher. Once we receive the hardware, it should take about a month or a month and a half to install.

Mr. Ostertag. You are speaking of the generators and synchronization?

Mr. Visher. Yes, and fitting it into the utility networks.

On pages 110 and 111 of the hearings, Mr. Thomas again raised questions regarding the cost of NEAR. Mr. Pittman estimated the federal cost would be $110 million unless they were forced into the purchase of receivers for installation in the homes.

The Committee also examined in some detail the estimate of $6,360,000 for protection of broadcast stations (p. 112 through 117). The civil defense estimates (inserted at page 117) indicated that the program covered three items:

1. A NAWAS drop at the station;

2. An emergency power generator;

3. A fallout-protected area at the transmitter location.

It was indicated that some 50 stations would be so equipped in Fiscal Year 1962 and the funds requested for Fiscal Year 1963 would complete about 900 additional stations. Most of the questioning revolved around the cost of the three items listed above.

Mr. Thomas. By the time you pay for your construction and your auxiliary power for 600 or 700 stations; what will that be per station?

Mr. Visher. This particular program is 100 percent Government contribution. They are providing the transmitters.

.....

Mr. Jonas. Since you are spending that much money building these shelters and providing this power, why do you not use that as your primary communicating link and cut out the telephone cost of $625,000 a year?

Mr. Visher. The AM broadcast band, which is the group we are talking about, the radio stations we listen to at 640, and 1240, these stations are not normally available to use to talk to regions, to talk to people on a warning basis. We need the basic communication link to talk and disseminate warning, disseminate vital information. It is not quite the same kind of link. One goes to every person via his radio, one goes to a specific point for use in time of emergency, and for normal operation of a system.....

In the Senate hearings on HR-12711, Mr. Pittman was questioned as to what programs would have to be postponed if the Senate went along with the House reduction.

Senator Saltonstall. There is a broad general question on this subject. The total you requested was $124,918,000 and the House allowed you $65 million, which left $59,900,000, which is the figure the chairman just brought out. Let me ask a broad general question. You divide it into eight different categories. If we went along with the House and did not give you any of this $59,900,000, would you go forward in a smaller way with all of these categories, or eliminate some of the categories?

Mr. Pittman. .....We would have to eliminate, I think, or postpone, a very substantial number of these eight projects.

Senator Saltonstall. If the chairman will permit me, let us very briefly, so as not to go into detail, cover this. You have warning and alerting, $25 million. Would you go into that in full?

Mr. Pittman. This, we believe, would have to be postponed a year. Whether we would completely postpone it or run several of the pilot projects is a judgment we have not yet made. But substantially it would be postponed.

.....

Mr. Pittman. I think then, to answer that question, if Congress decides to defer the survival capability I refer to in my opening statement, we have to postpone, or eliminate from this budget completely, some of the priority elements here and go ahead and do others as completely as we can. In this case I think that most of the NEAR operation would have to be postponed. The first one.

Senator Saltonstall. All right. The second one we have already talked about at some length.

Senator Magnuson. No. This is for radio broadcast stations.

Senator Saltonstall. Yes. Needed for Government authorities to communicate with the public immediately following an attack. That is a different one than you have here.

.....

Senator Saltonstall. Would that be top priority or not?

Mr. Pittman. I think it is one we would be forced to put off a year.

Independent Offices Appropriations for 1964

Questions raised by the committee members of the House concerned principally the Emergency Broadcasting system and NEAR.

Mr. Thomas. What shape are we in with regard to this field? You have your radiological fallout detection and monitoring, warehousing and maintenance, but what about your warning and alert system? You made a little change recently, did you not? Your changed CONELRAD, but what did you put in its place?

Mr. Durkee. Mr. Chairman, CONELRAD was not an alerting system.

Mr. Thomas. Yes; that was your communication system.

Mr. Durkee. It was a communication system. It has been converted into an Emergency Broadcasting System. The major effect of the change is to increase the capacity of the country to use present radio stations for emergency information in a nuclear attack. With the FCC and with the industry we have created an Emergency Broadcasting System of 1,369 stations, I believe the number is. The function of these stations would be to broadcast emergency messages of the President or a designee of the President.

Mr. Thomas. They are going to let you break in for that purpose.

Mr. Durkee. Used only for those purposes.

Mr. Thomas. You are not going to pay anything for it?

Mr. Durkee. The budget provides for the hardening of a selected number of those stations for fallout protection.

Mr. Thomas. What do you mean by that?

Mr. Durkee. In order for--

Mr. Thomas. How did you protect each station? You may just as well try to protect a needle in a haystack; is that about right?

Mr. Durkee. Assuming the fallout program, as Mr. Pittman described it--

Mr. Thomas. There is nothing new in the idea of hardening those stations. You came up with that 3 or 4 years ago, did you not?

Mr. Durkee. Our program for hardening broadcast stations to provide fallout protection started in Fiscal Year 1962. It is perfectly clear that if you are going to protect the country against fallout, you have to protect also the means of communication during this period. What we are proposing to do and have done already is to protect the broadcasting station personnel from that same fallout so that the President can use the system.

.....

Mr. Durkee. ..... In 1964 we propose to harden 83 stations and to provide 105 with emergency generators and radio program links.

.....

Mr. Shipley. The FCC selects the station jointly with you?

Mr. Durkee. That is right.

.....

Mr. Shipley. What about the broadcasting equipment? In other words, if you select a station and they lack the necessary equipment, would you go in with FCC for the supporting equipment?

Mr. Durkee. The fallout protection is the barrier shielding, and we are providing them with emergency power if the power should disappear.

Mr. Shipley. Give me again the first part.

Mr. Durkee. The barrier shielding that would protect the operating personnel.

Mr. Shipley. I mean specifically the broadcasting equipment.

Mr. Durkee. The only broadcasting equipment is the radio broadcasting equipment that would link the broadcasting station with the Governor or the mayor or those who would use the station in an emergency.

Mr. Shipley. This is a nominal cost, is it not?

Mr. Durkee. $289,000 for 105 stations, or an average cost of $2,753 (p. 958, 959, 960).

The justification for the NEAR system is included on pages 960-961 of the hearings. This material indicates that with the 1962 funds of $5.1 million, four contracts for eight NEAR receivers were awarded. Contracts were also let for prototype production of NEAR receivers. In 1963, funds available were used for consulting and engineering services ($1.1 million), 16 converters ($2.4 million), and a special installation at Phoenix, Arizona, ($42,500). The funds requested for 1964 would provide for $900,000 for services and $3.6 million for installation of NEAR converters to complete

the NEAR system in lower Michigan and to provide the initial phase in establishing a system covering the Washington, D C. area.

The discussion of the NEAR system is included on pages 960 through 967 of the House hearings. Pertinent comments were as follows:

> Mr. Thomas. You are past the experimental stage?
>
> Mr. Romm. No, Sir. We now have three of these generators installed, one in Columbia, Mo., one in Phoenix, and one in Colorado Springs.
>
> Mr. Thomas. You want to install four more?
>
> Mr. Romm. From 1962 funds, we will install 5 more, 16 with Fiscal Year 1963 funds, and 19 requested for Fiscal Year 1964. When the entire nationwide system is installed, we will have the ability to sound an alert to the entire population at the same time with this system.
>
> .....
>
> Mr. Thomas. Why is not that system you have now pretty good? You know it will work?
>
> Mr. Romm. It does not give you complete coverage. The current system ends in an outdoor siren system, and does not give indoor coverage and does not give coverage for the population as a whole.
>
> .....
>
> Mr. Shipley. I have witnessed mock attacks over the past several years, and have listened to them blowing the siren 5 minutes or 2 minutes, and then quiet, and it was all worked out a week in advance, and yet if you can get 20 people to know what is going on, it is terrific. I think they have failed dismally in the warning system. The thought has occurred to me that for a warning to be given in every home in the country--and I am not promoting the telephone company--but why could not each district telephone office have a system of ringing the phone constantly?
>
> Mr. Pittman. A full review of alternatives has been going on, using radio and every system in use. The telephone is out, for technical reasons; the load that would have to be

carried on simultaneously is too great. Where we stand is this: We agree with you that the outdoor warning system is entirely inadequate. It is inadequate from the standpoint of coverage, and it is inadequate also in that it does not produce the effect on people that gets the response that is needed unless people know it is a real emergency, and they may or may not know that.

Mr. Thomas. What happened to that gadget you were experimenting with that you attach to your telephone?

Mr. Pittman. This probably preceded our time, but there may be people in the room who are familiar with it. Whatever happened to it, it was thrown out. Does anybody want to suggest why?

Mr. Romm. I know of no telephone gadget considered in recent history. You may be thinking of the NEAR receiver which plugs into an electrical outlet.

.....

Mr. Pittman. Yes, the receiving end will be a low-cost, small black box that gives a signal.

Mr. Thomas. That is what I was thinking of. How is that coming along?

Mr. Pittman. On the black box there is procurement of 100,000 and it looks like it is in good shape. On the generators, the development is in good shape. The problem is to demonstrate to the utility companies as well as to ourselves that it works on a system basis and that it will not interfere with other peacetime operations.

Mr. Thomas. You are not throwing your siren system overboard? What are you spending on the experimental system?

Mr. Romm. We had $5.1 million in 1962 and $3.5 million in 1963.

Mr. Thomas. What does it look like to you?

Mr. Romm. It looks very good. The generators we have tested did not interfere even with the most sensitive systems. In fact, we have worked with people who

operate computers where very minor power differences will throw computers off, and we have found the generators will not interfere even with the computer operations.

.....

A general discussion of the warning system followed, which brought out the following facts:

The yearly operating cost of the warning system was $1.7 million which was now budgeted by the Department of the Army.

The $5 million included for 1964 covered $4.5 million for NEAR and $500,000 for the Washington area warning system.

About 60 million receivers would be needed for the NEAR system.

In a further disucssion of NEAR, Mr. Thomas indicated there was quite an engineering problem and asked the civil defense witnesses when they thought they would come up with the correct answer. He also indicated that it was a highly technical matter, and asked if when civil defense came before the committee the next year, if the matter would be settled one way or the other. Mr. Pittman indicated that they were planning on the end of Fiscal Year 1963 as the time when there would be enough data for a decision as to whether to go ahead with the entire system.

The questioning of the Committee on the Emergency Broadcast System is covered on pages 967 through 972. The first part of the questioning had to do with the number of broadcast stations, the number included under the system, and the number to be hardened. The narrative on Civil Defense's justification of this program is included on pages 969 and 970 of the hearings. The hearings included the following comments:

Mr. Thomas. How much time will you have anyway? What if you had a dozen systems?

Mr. Pittman. For a program designed primarily to provide fallout protection--

Mr. Thomas. You have to be alive first.

Mr. Pittman. But an important part of the problem is those who are outside of the holocaust and have a chance of surviving, and they have 30 minutes at least. Also, I would like to make clear there is a difference between

warning and communications. We cannot use our emergency communications without triggering it. We have to get people to turn their radios on.

.....

Mr. Ostertag. Under your program of providing shelters, that is more or less on a grant basis, is it not, for buildings and communities and institutions and the like? Why should the civil defense organization of the federal government be responsible for 100 percent of this hardening protection of the stations? Even though they do render a service, they benefit from that protection as a private corporation or private institution.

Mr. Durkee. Let me make clear what we are protecting. We are only protecting a small number of operating people. It is only to keep a capacity for the federal government to use this system and have the people there to run it. There is no public sheltering for the public at large, either for the station personnel or the public at large.

Further questioning covered how the stations were selected for inclusion in the net, and the nature of the protection afforded. It was brought out that the FCC participated in the selection of the stations, and that participation by the stations in the program was voluntary.

In the Senate hearings on HR-8747, the prepared statement of the Office of Civil Defense covered justification for $4.5 million for NEAR, $500 million for the Washington area warning system, and $2 million for broadcast station hardening. (p. 1410-1411, Part II). Office of Civil Defense budget justification for NEAR was included in the hearing record at page 1436, and that for hardening broadcast stations at page 1439. The principal discussion in the Senate concerned the NEAR system. Again, the questioning mainly involved the problem as to who was going to pay for the system.

Independent Offices Appropriations for 1965

Part 2 of the House hearings covers the appearance of FCC witnesses in support of Executive Order 11092 which gave that agency certain responsibilities in emergency planning (p. 1444 through 1453). Mr. Thomas raised the question as to why CONELRAD had been changed.

Mr. Bartley. We will have greater coverage through the new plan which becomes effective June 30. Prior to that time they operated on 640 or 1240. The Department of Defense, as the result of a review, determined there was no longer that requirement.

Mr. Thomas. What was the basis of their assumption that it was no longer needed?

Mr. Bartley. That I do not know.

Mr. Solan. Was it not because the planes would not be homing on radio signals?

Mr. Bartley. It was their determination.

Mr. Thomas. I was wondering what the basis was. We are out of the bomber area into the missile area, is that it?

Mr. Bartley. I think it is the more sophisticated navigation aids on the planes themselves so we can allow the stations on the air to operate with existing coverage and thereby provide a more flexible system. We have a statement of requirements from the press secretary of the White House as to Presidential needs.

.....

Mr. Bartley. So now, come June 30, to meet the Presidential requirements we must continue the emergency broadcast system development. This is the part that has been paid for originally by the Air Force and this year by OCD.

.....

Mr. Thomas. May I interrupt you there? What you are directing your remarks to is postattack, and we have gone into this before. What can we put on the record about our early warning system?

Mr. Bartley. I am not at all qualified, Mr. Chairman, to talk about it. I do not know.

Mr. Ostertag. The chairman has pointed up one emergency, postattack, but what I was trying to determine, in the planning and in dealing with communications generally, which is a vital part of our lifeblood in this country, there are many kinds of emergencies and I wondered if there is a relationship between one kind of disaster as against another in which you have problems in this field whether it be before or after the emergency.

Mr. Bartley. I was about to say that as a result of his calling on the stations in the Alaska area they had some plans for a national emergency which were used immediately in the Alaska disaster as well. Radio stations had auxiliary power. They got back on the air in about 10 minutes. So that I am sure this had a tremendous impact on the manner in which the public behaved under those conditions. They did have authentic information coming to them.

.....

The hearings on the civil defense budget were highlighted by the fact that the Committee was told that NEAR was to be put on the shelf. (p. 1504 through 1509).

Mr. Durkee.....In the area of warning and detection we have made a decision that you asked about last year, as I recall "What are you going to do about the NEAR warning system? When will you come to a decision about that?"

I am here to advise you a decision has been made that we will not spend any more money on that for these particular reasons:

(1) With the money that has been spent we have developed a shelf item that could be deployed if needed.

(2) It seems we should not spend more money in developing powerline systems such as NEAR because technological developments and the discontinuance of CONELRAD indicate there are other warning systems possible that might be cheaper or more effective. We intend to spend about $1.1 million during Fiscal Year 1965 on radio indoor warning systems, and I hasten to add they include not only the standard broadcast type but also Government systems such as the Loran C navigation system. There is a wide range of possible radio warning systems.

We have also explored the use of the telephone as a warning system. An estimate by A.T.&T. in 1962 was that from $6 to $7 billion dollars would be involved in modifying the telephone system to a warning system, so for the time being we have discarded that as an idea. .....

I might add that we have turned over the administration of our national warning system--that is, the funding of it--and also our radio and telephone communications to state

governments, to the Army under the supervision of the Defense Communications Agency. The Army budgets the cost, which is about $4 million annually. This does not show in our budget. That, I think, pretty well covers the system on warning and detection.

.....

Mr. Jonas. We spent $4 million on this NEAR warning system so far, is that right?

Mr. Durkee. Historically about $8 million has been spent.

Mr. Jonas. I mean in 1963 and 1964?

Mr. Durkee. Yes, Sir. .....

Mr. Jonas. What do we have for this $8 million?

Mr. Durkee. For the $8 million you have a powerline warning system, that is, detailed workable specifications for the generators that would run this system and the warning receiver.

Mr. Jonas continued his questioning regarding NEAR and its testing in lower Michigan. He continued with questions on the effectiveness of NEAR:

Mr. Jonas. Are you far enough along with operations to test the effectiveness of it?

Mr. Durkee. Yes, we have had a number of testing operations.

Mr. Jonas. And you can tell the committee that the testing so far discloses that the system is workable, effective, and efficient?

Mr. Durkee. Yes.

.....

Mr. Jonas. You can see that I am trying to put on the record a statement which will give us some idea of what it will cost to put in this warning system in every city in the United States.

Mr. Durkee. I believe what I have said about these other systems is relevant, Mr. Chairman, that the radio systems on which we are planning to spend very little money to develop will be much less expensive to deploy around the country, which is one reason for going no further with this system.

Mr. Jonas. You mean you have abandoned the system you started out with which has been described as the "little black box" system?

Mr. Durkee. I want to say very clearly it has not been abandoned. It is a system that has proven workable. The reason we would not make any decision now to deploy the NEAR system is that there are other more effective ways to do that which result from technological developments in radio.

Mr. Thomas. Spell that out a little bit for us.

Mr. Durkee. I have the technical experts here but what is involved here is using radio and a radio receiver that will be in a home which could be alerted by the national warning system and a buzzer sound which would mean a warning.

.....

Mr. Durkee. There is one system that would operate in a regular radio receiver with the transmission being interrupted by a sound signal. There are other radio systems that we are looking at that would not be the commercial radio-type system but they are radios in which you would have to buy a special receiver which would give you not only signals but also a voice over the receiver. One of the reasons this has never been pursued in the past was because the radio receiver costs were so high. Technology has reduced the cost to where they are equal to the cost, for example, that would go in a little black box.

Mr. Jonas. I thought the little black box concept was brought into being by acceptance of the fact that many people do not have their radios on all the time. You have to have some way to alert a housewife that she ought to turn her radio on.

Mr. Durkee. That is right. One of the radio systems would automatically turn the radio on. The cheapest radio warning system you could use which we have looked at is an ordinary radio receiving an ordinary program with a warning signal being given over that radio by means which would increase the volume by a great amount. In other words, you might be listening to music and the warning signal would be an enormous increase in volume.

Mr. Thomas. As Mr. Jonas pointed out, suppose the radio is off and it is in the dead of night. You mean you have a device that would turn it on?

Mr. Durkee. Yes. It would not be a commercial radio.

Mr. Jonas. It would involve everybody buying a new receiver?

Mr. Durkee. Yes.

Mr. Jonas. What would it cost?

Mr. Durkee. The total cost of the receivers would be about $1 billion.

Mr. Jonas. I mean per each?

Mr. Durkee. About $10; it would range between $10 and $12.

.....

Mr. Jonas. It would have to be a pretty loud noise to wake up some of the sound sleepers. The receiver may be downstairs in the living room and the people are upstairs in the bedroom sleeping with the door closed.

Mr. Durkee. The system is the ordinary radio which is broadcasting music, for example, and the volume is turned up.

Mr. Jonas. I understand that, but this radio is completely off.

Mr. Durkee. It would not work if the radio is completely off. Another system is turning on what is in effect a radio-like box even if it is off. We are looking into the entire range of technical possibilities. All of these involve a receiver cost but the first does not involve a

receiver cost in the sense that all those that have radios now have it if the system is put in.

.....

Mr. Jonas. What do you plan to spend in total for warning systems in further expenditures?

Mr. Durkee. We are planning on spending $1.1 million in this budget and that should do the job. I am using $500,000 of 1964 year funds for the same purpose. So a total of $1.6 million will have been spent at the end of Fiscal Year 1965 on the final look at the radio warning system.

Mr. Jonas. So far as you are concerned you think that will do the complete job and there will be no further money requested in the future? Of course you cannot bind anybody, but is that your present thinking?

Mr. Durkee. We will continue to expand the warning system we have now and I have budgeted money for certain activities in relation to our warning points. I am not recommending at this time any budget for any other warning system except the one we have and its expansion.

Mr. Jonas. You mean the one in Michigan?

Mr. Durkee. No, the national warning system from our federal warning offices to the state, and they are linked with the sirens in your community.

Mr. Jonas. You expect to put the Michigan system on the shelf, so to speak?

Mr. Durkee. That is right.

.....

The Emergency Broadcast System was discussed next (p. 1509, 1513, 1514):

Mr. Durkee. .....The next series of items are "Emergency operations." The first is the emergency broadcast system. Our role in the emergency broadcast system is a small one. ... The major responsibility in terms of administration and management is that of the Federal Communications Commission,

and I believe Commissioner Bartley appeared before you to cover that subject. Our budget proposal of $5.5 million relates to the creation of fallout protection for the operating personnel of these emergency broadcast system stations. It is a program we discussed last year and we are asking for funds sufficient to provide fallout shelter protection for 465 stations. We asked for and received approval for fallout shelter protection for 90 stations last year.... The emergency broadcast system should not be confused with the use of radio for warning. Emergency information is a continuing operation both during a nuclear attack and before and after a nuclear attack.

.....

Mr. Jonas. I am not quite satisfied from what you said about the justification for this emergency broadcast system. What is it exactly you propose to do? I thought the President of the United States could get a 150-million audience by merely calling up 2 people to make all television and radio facilities in the country available. What is it you propose exactly to use for this $8 million for an emergency broadcast system? I want him to have what he needs, and I think the people want him to have what he needs, but I am wondering if he needs it, in addition to what is already available.

Mr. Durkee explained the reason for the creation of the emergency broadcast system and then indicated how the requested funds would be used:

What we are proposing to do is a very small part of that system. We are proposing to create fallout protection for the operating personnel, two or three or four people that would be necessary to keep that station in operation during an actual attack and after the attack. The average cost of doing that per station is about $5,000. We would also be asking for funds to put emergency generators in those stations and program radio links to mayors and Governors so they can use the broadcasting stations for state and local purposes.....

Mr. Jonas. $300,000.

Mr. Durkee. The $300,000 requested by the Federal Communications Commission is to support personnel to create through the mechanics of the system, how these stations relate to each other and what stations are in the system.

The $5.6 million is for the purpose of creating fallout protection for the operating personnel of 465 of these stations. Without that protection, in an actual nuclear attack the station personnel would have to leave the premises, go to public fallout shelters, and you would have no radio broadcast system operating at all.

Mr. Jonas. You are going to provide fallout protection in the stations for a limited number of people?

Mr. Durkee. That is correct....

Mr. Jonas. That is sort of callous. If I were running a station and somebody came in and wanted to build a shelter to protect only five of my people, I would feel a little obligation to provide similar protection for everybody there.

Mr. Durkee. This is not the first year this has been requested, Mr. Congressman. Money for 90 stations was authorized last year and in the previous 2 fiscal years. This program is administered by the Corps of Engineers. It is a successful program. The station owners understand what this is for. There is not a great deal of publicity about it. It is not creation of public fallout shelters.

.....

There was a further discussion on the use of emergency generators and Mr. Durkee illustrated their benefit by discussing their use during the Alaska earthquake (p. 1514, 1515).

Later in the hearings (p. 1526-1528), Mr. Thomas inserted in the record OCD's justification for research on warning and alert, but there was no discussion on this item.

.....

The Senate hearings on this bill (HR-11296) contain at pages 911 through 915 the prepared statement of the Office of Civil Defense in justification of its requests for restoration of funds deleted by the House. A discussion of the emergency broadcasting system and the warning system is covered on pages 928 through 935 of the hearings. OCD in response to questions, indicated that 656 stations were to be provided with fallout protection at

an average cost of $5,000, that the cost of a generator was about $8,000, and the cost of program links about $2,000. There was also a discussion on the nature of the program links:

> Senator Magnuson. Now the line, why would it cost so much for a line? There may be a good reason for it.
>
> Mr. Durkee. It is about $2,000.
>
> Senator Magnuson. When there is a line from every radio station to the city hall or the fire department or to any place. There is a line there.
>
> Mr. Durkee. Well, they are generally not lines of the kind we are talking about. This is a direct line that allows the mayor for example to broadcast over that radio station from the city hall.
>
> Senator Magnuson. This is a local line?
>
> Mr. Durkee. It is really a local hotline. It goes right into that radio broadcasting station.
>
> .....
>
> Senator Magnuson. And they would have to all have lines into a separate given central point.
>
> Mr. Durkee. That is right.
>
> Senator Magnuson. Who lays down these lines? What do you do, rent them from the telephone company?
>
> Mr. Durkee. Yes; the current wire lines are rented, but they are being taken out as radio equipment for these programming links as installed.
>
> .....
>
> Senator Magnuson. $2,000 sounds a little high if you are just leasing lines, but if you have to add some construction equipment-----
>
> Mr. Durkee. I am sure there is an installation cost in doing it.

Senator Magnuson. Then it wouldn't seem high.

Mr. Durkee. That is right. I am sure there is an installation cost.

Senator Magnuson. You might have to add something that the phone company wouldn't have.

Mr. Durkee. Wouldn't have, yes.

Senator Magnuson. But I think the record ought to show that.

Mr. Durkee. We will be glad to have the record show that, Mr. Chairman.

Civil Defense Emergency Broadcast System (EBS)
Communications Lines

The communications lines used under CONELRAD for alerting the radio stations and programming at local levels was continued for the emergency broadcast system upon discontinuance of CONELRAD. These facilities were financed by the Department of the Air Force, and on July 1, 1964, the Department of the Army takes over the financial responsibility based on the continued need.

The Fiscal Year 1964 costs for the interconnections to the AP/UPI alerting system is approximately $98,000. The costs for the telephone lines for programming local radio stations by local civil defense authorities is approximately $109,000, or about $9,000 a month.

As the OCD broadcast station protection program is extended to more stations, remote radio pickup (RPU) equipment procured by OCD being installed between the local Civil Defense Emergency Operations Center and the radio station will eliminate the need for the local telephone circuits. The complete installation of RPU equipment is costing about $2,700 per station. This will result in added reliability for emergency programming to the civilian population and savings in rental costs currently paid to telephone companies.

.....

Senator Allot. How would you get all the radio stations off the air, for example, except the ones that you have selected?

Mr. Durkee. The system to get them off the air is a relatively simple system. At NORAD when an air raid warning is declared, there is an automatic triggering of the emergency broadcasting system at the same time that warning is sent over the national warning system. A special interconnection will seize the AP and UPI teletype news facilities to the radio stations. They will receive a message which tells them either to stay on the air or get off the air in accordance with the EBS plan. There is a regular emergency procedure in effect at all broadcasting stations so that this would happen in the matter of about 5 minutes, so that technically it certainly will work.

There followed a discussion of what coverage was available on a 24 hour basis at the end of the warning line to make decisions on the basis of the warning received.

Senator Magnuson. It will end up in some radio station.

Mr. Durkee. No sir. I am now talking about something a little different. The emergency broadcasting system is one thing, which is a way of handing emergency information. It is triggered at the same time the air raid warning is disseminated over a separate system. This is the OCD national warning system from NORAD which sends out a warning signal through our 600 warning points all around the country simultaneously and this goes out in a matter of minutes.

.....

Senator Magnuson. Who is at the end of that, your people?

Mr. Durkee. No; the state or local civil defense people, and whoever the mayor has appointed to handle this kind of problem.

Senator Magnuson. Twenty-four hours a day?

Mr. Durkee. Twenty-four hours a day.

Senator Magnuson. Who pays for that?

Mr. Durkee. We pay for the installation of the national warning system, and we pay part of the cost of the installation and maintenance of state and local systems through matching funds.

.....

The elimination of CONELRAD was also discussed:

Senator Allot. You have done away with these two emergency channels; is that right?

Mr. Durkee. That is correct.

Senator Allott. What is the reason for that?

Mr. Durkee. The original reason for the imposition on the broadcasting industry of these two channels was a military reason, because of navigational aid to an incoming enemy aircraft. With the advance of technology in other navigation systems for both missiles and aircraft we were able to get rid of those restrictions on the use of radio and in effect the whole spectrum of radio broadcasting is now open for emergency purposes.

Senator Allott. To stay on its regular frequency?

Mr. Durkee. Yes, Sir.

.....

Senator Magnuson. You wouldn't be a homing device.

Mr. Durkee. That is right.

Senator Magnuson. Technologically?

Mr. Durkee. Technologically it isn't a problem, for military reasons.

Senator Magnuson. For aircraft or anything else?

Mr. Durkee. That is right.

Senator Allott. I don't see that that makes any difference, frankly, because for example KOAX, 830 on the standard broadcast dial, and anybody using a plain ADF can flip it to 830 and they could home in on KOAX from a distance up to 400 or 500 miles I would think.

Mr. Durkee. Yes; but I gather because of the advance of navigation itself, and, of course, the development of missiles, the problem simply isn't the same any more.

.....

The final item on warning discussed in the Senate hearings concerned testing of the outdoor warning system:

Senator Magnuson. Who determines when the sirens blow when there is not an emergency. That is a local decision?

Mr. Durkee. A local decision.

Senator Magnuson. And you have nothing to do with that?

Mr. Durkee. No.

Senator Magnuson. Because there I think indirectly you are getting into exactly the problem he mentioned. They keep blowing and blowing and blowing, so that nobody pays any attention to them.

Mr. Durkee. We have suggested, Mr. Chairman, that they stop doing that, and that they select one specific time which is consistent throughout the state, to have these sirens go.

Senator Magnuson. They don't need to blow them at all until something happens.

Mr. Durkee. Not very much.

Senator Magnuson. They don't need to blow them.

Senator Allott. They have got to be sure they work.

Mr. Durkee. They have to test them occasionally to be sure they work.

Senator Magnuson. They can tell whether they work without blowing them all the time.

Mr. Durkee. I think there was a time when they were more primitive than they are now when you might have had to do it a lot more.

Senator Magnuson. It is like the old Navy story about fire in the galley, you know.

Mr. Durkee. Yes. Mr. Chairman, there are a couple of critical items here.

Senator Magnuson. Anyway, that decision is made by the local people.

Mr. Durkee. That is correct.

Independent Offices Appropriations for 1966

In the House hearings on civil defense appropriations for Fiscal Year 1966, the discussion on warning is included on pages 614 through 618. Excerpts from the civil defense budget on warning were inserted in the record and appear on pages 635, 636, and 641 through 644. The Committee members raised questions on NEAR:

Mr. Jonas. How about your little black boxes?

Mr. Durkee. We are not asking for any money this year for the NEAR program which has the little black boxes. This year we are conducting final tests using money appropriated during Fiscal Year 1964.

Mr. Jonas. Do you have any in place?

Mr. Durkee. Yes. We have some in a test in Michigan. This is a test of the NEAR system that we discussed last year.

Mr. Thomas. What did you spend on the little black box program?

Mr. Durkee. $8.5 million.

Mr. Thomas. Did that include research?

Mr. Durkee. That included the research. Those were the total developmental costs.

Mr. Thomas. There is one thing about it, Mr. Jonas, the older a program gets the less you spend on it. Some costs have gone down 66 percent.

Mr. Durkee. I hope your comment was not one of skepticism but of pleasure, because that is what is happening.

Mr. Thomas. I wonder why we made that serious error to begin with.

Mr. Durkee. It may not have been a serious error. The reason the NEAR system was developed was because the radio warning system was not available.

There followed a description of the warning system and the EBS. Mr. Durkee mentioned that money had been spent to protect 530 selected radio stations, and that the total cost would be $10 million. The problem of getting the warning down to the local level was discussed as was the use of the outdoor sirens. The question of a better system was raised in the following discussion:

Mr. Thomas. What is a better method of alerting them. Your black box did not work.

Mr. Durkee. The black box would work, Mr. Chairman. I do not think it is the best system. We think the best system will be a radio warning system that would activate a radio receiver in a person's home.

Mr. Thomas. Even though the radio set is turned off?

Mr. Durkee. Even though the radio set is turned off.

Mr. Thomas. How far along are you with that?

Mr. Durkee. I have just gotten a recent report and I would say all the technological reports so far show this is feasible and cheaper and I have prototypes of the kind of radio receivers that would be used. We are working with the FCC and the radio broadcasting industry and we have a task force working on it.

Mr. Jonas. That might work in homes but business concerns and factories and commercial establishments do not all have radios.

Mr. Durkee. A number of them have regular radio services. Also, some companies have done what Marshall Field has done in their building in Chicago. They have a line connected to the national warning system in their own building.

Mr. Jonas. They are, in effect, a warning point?

Mr. Durkee. A warning point extension.

Mr. Giaimo. Is this telephonic?

Mr. Durkee. Yes; telephonic, a land line, A.T.&T. wire. There is an actual linkage in the building that comes from NORAD and they would get the warning in a minute or minute and a half.

Mr. Thomas. Is there any way to sabotage the big center so that the message cannot get through? Could not that be easily sabotaged?

Mr. Durkee. There is a redundancy of lines for this system as for telecommunications, and there would be top priority given to circuit rerouting and restoration. I do now know off the top of my head what the extent of the sabotage would have to be before it would be inoperative.

Mr. Jonas. I do not think there would be much trouble getting the information around in a small town if it gets to the town in time. If John Jones runs off with Susie Smith everybody knows about it in 15 minutes.

Mr. Durkee. You have about 30 minutes before radiation starts coming down. Let us assume many small towns would be so located that the first fallout would not arrive until 2 hours later. They have considerably more time than the 30 minutes and radio communications would bring the news.

Mr. Jonas. Would not that depend on how far the town is from the blast or explosion?

Mr. Durkee. Yes. That is why I say if you are planning on doing something you had better plan on 30 minutes. You had better not plan on 2 hours because you might not have that time.

.....

Mr. Jonas. Mr. Chairman, can you give us the total cost of this warning system, including what the Army Strategic Communications Command budgets?

Mr. Durkee. Yes.

Mr. Jonas. What would that add to this?

Mr. Durkee. The warning system. That adds about $1.3 million for Fiscal Year 1966 for the warning system.

Mr. Jonas. You are sure you are not overlapping there?

Mr. Durkee. No. The specific budget amount is worked out with them every year. They maintain the system for us and budget separately for that. They programmed $1,265,000 during Fiscal Year 1965 for the maintenance of the warning system.

.....

A discussion of the Bomb Alarm System followed. It was pointed out by the civil defense witness that this was not a part of the civil defense warning system. A summary on the system appears on page 640 of the House hearings.

In the 1966 House hearings on the FCC appropriations, mention was made in the prepared statement (p. 843) of the FCC role in the Emergency Broadcast System, but there were no questions raised in the hearings.

ANNEX IV TO CHAPTER THREE

FISCAL HISTORY OF CIVIL DEFENSE WARNING SYSTEMS

Table 3-1. Warning Obligations - Fiscal Years 1951 Through 1964

Obligation[1]	Amount
Federal Contributions for Warning	$ 19,178,192
Emergency Broadcast System	5,586,881
NEAR	9,412,693
NAWAS	6,650,028
WAWAS	2,857,348
NAWAC	223,349
CADW System	716,532
Radio Indoor Warning System	646,187
Fallout Protection for Warning Points	95,425
Research-Warning	2,613,005
Total	$ 47,959,640

1. Total obligations 1951 - 1964: $1,082,825,648; Percent of warning obligations to total obligations: 4.4 percent.

Table 3-2. Comparison of Total Funds Requested and Those Appropriated vs. Selected Warning Funds Requested and Those Obligated

Fiscal Year	Total Funds Requested (Millions)	Total Funds Appropriated (Millions)	Percent	Warning Funds Requested (Millions)	For *	Warning Funds Obligated (Millions)	Percent
1951	$ 403.0	$ 31.8	8	$ 5.6	FC	$ 0	0
1952	537.0	77.0	14	4.2	FC	2.7	63
1953	601.6	44.3	7	4.75	FC	.97	20
1954	153.3	49.3	32	12.0	FC	2.15	18
1955	88.5	50.2	57	1.3	FC	1.02	78
1956	78.8	70.9	90	1.0	FC	.95	95
1957	125.5	95.8	70	1.7	FC	1.19	70
1958	132.4	41.6	31	1.5	FC	1.62	107
				.75	R	.60	81
1959	76.5	45.3	59	1.8	FC	1.57	87
				1.1	R	.04	4
1960	101.7	52.9	52	.95	FC	1.09	114
1961	77.3	61.1	79	1.46	FC	1.25	86
				.16	R	.02	15
1962	312.1	294.2	94	.88	FC	1.53	173
				.02	R	.07	372
1963	756.9	128.0	17	6.4	EBS	1.11	17
				25.0	NEAR	3.45	14
1964	346.9	111.6	32	1.98	EBS	3.69	186
				4.5	NEAR	.72	16
1965	358.0	105.2	29	5.58	EBS	3.74	67

*FC - Federal contributions to match state and local funds for warning.
R - Warning research funds.
EBS - Emergency Broadcasting System
NEAR - National Emergency Alarm Repeater System.

Table 3-3. Obligation History of National Warning System (NAWAS and Predecessor Systems)

Fiscal Year	Annual	Cumulative
1957	$ 223,349 (NAWAC)	$ 223,349
1957	716,532 (CADW)	939,881
1958	1,073,957	2,013,838
1959	1,136,984	3,150,822
1960	1,173,727	4,324,549
1961	1,334,633	5,659,182
1962	1,486,216	7,145,398
1963[1]	424,511	7,569,909

1. Transferred to U. S. Army during FY 1963.

Table 3-4. Obligation History of Washington Area Warning System (WAWAS)

Fiscal Year	Annual	Cumulative
1958	$1,055,293	$1,055,293
1959	561,536	1,616,829
1960	332,059	1,948,888
1961	165,028	2,113,916
1962	230,425	2,344,341
1963	187,847	2,532,188
1964	325,165	2,857,353

Table 3-5. Obligation History of Warning - Matching Funds

Fiscal Year	Warning	Cumulative
1952	$2,676,230	$2,676,230
1953	969,378	3,645,608
1954	2,155,487	5,801,095
1955	1,016,751	6,817,840
1956	953,513	7,771,359
1957	1,193,874	8,965,233
1958	1,615,565	10,580,798
1959	1,571,629	12,152,427
1960	1,087,623	13,240,050
1961	1,250,135	14,490,185
1962	1,527,871	16,018,056
1963	1,962,013	17,980,069
1964	1,198,123	19,178,192

Table 3-6. Obligation History of Emergency Broadcast System

Fiscal Year	Annual	Cumulative
1962	$ 278,809	$ 278,809
1963	1,106,783	1,385,592
1964	3,689,632	5,075,224

Table 3-7. Emergency Broadcast Systems: Other Government Agency Support

Fiscal Year	Corps of Engineers	FCC Personnel	Annual	Cumulative
1962	$ 43,587		$ 43,587	$ 43,587
1963	85,475		85,475	129,062
1964	147,595	$235,000	382,595	511,657

Table 3-8. Obligation History of National Emergency Alarm Repeater (NEAR) System

Fiscal Year	Annual	Cumulative
1960	$ 29,840	$ 29,840
1961	87,114	116,954
1962	5,117,792	5,234,746
1963	3,453,188	8,687,934
1964	724,759	9,412,693

Table 3-9. Obligation History of Radio Warning System

Fiscal Year	Annual	Cumulative
1964	$646,187	$ 646,187

Table 3-10. Obligation History of Fallout Protection for Warning Points

Fiscal Year	Annual	Cumulative
1964	$ 95,425	$ 95,425

Table 3-11. Obligation History of Warning Research and Development

Fiscal Year	Annual	Cumulative
1956	$358,000	$ 358,000
1957	106,000	464,000
1958	604,000	1,068,000
1959	42,000	1,110,000
1960	-	1,110,000
1961	3,000	1,113,000
1962	742,000	1,855,000
1963	185,000	2,040,000
1964	331,000	2,371,000

Chapter Four

Strategic Warning to Industry

1.0 INTRODUCTION

This chapter contains the preliminary findings of a study on providing strategic warning to industry.[1] The objective of the study was to investigate the time requirements and the costs involved in an emergency industrial shutdown. The study was also intended to determine the feasibility of providing strategic warning to industry in a crisis situation. Because of problems in obtaining information from various industries in the short time available for the study, only preliminary work was completed. Based upon the initial findings of this investigation, a tentative evaluation was made of the trade-off between shutdown and possible escalation of a crisis, and the failure to shutdown and probable damage or destruction of various plants and the communities surrounding them. Of prime importance in the evaluation was the consideration of the potential consequences of a strategic warning false alarm.

Within the limited scope of this activity, coordination was effected with personnel at the Stanford Research Institute (SRI), who are concerned with the execution of the concurrent OCD-funded project to evaluate the effectiveness of shutdown procedures in key industries. The SRI project and this industrial warning study were conceived to be mutually complimentary efforts. Experience to date confirms the interrelationship of the two projects.

The time available for study was short, and the sources of shutdown information limited. Thus, many problems are posed to which this chapter offers no solutions. This is not to say, however, that solutions do not exist. The primary purpose to the chapter is to point up the potential problem areas, and to show the need for further consideration of them.

2.0 CONCLUSIONS AND RECOMMENDATIONS

The conclusions which emerged during the course of the preliminary study reported in this chapter are as follows:

1. Limitation upon Tactical Warning. Under present concepts, the allowable reaction time to a tactical warning is between 15 minutes and a half hour in target areas. Estimates of shutdown time requirements indicate that shutdown could not, in a number of significant cases, be accomplished within this time frame. It can be seen,

1. This chapter replaces Industrial Warning, which was originally published as TM-L-1960/083/00, dated 14 January 1966.

however, that in certain key industries, such as petroleum and steel, complex production equipment will destroy itself, and, in some cases destruction of this equipment will probably result in the destruction of surrounding areas if the processes are not shut down. Thus, if the effect of a hostile attack upon the industrial capability of the nation is to be minimized, then warning and shutdown procedures must be developed to maximize the survivability of those industries not directly affected by the attack.

2. Level of Public Preparedness. The feasibility of giving industry strategic warning is dependent upon how the public would respond to it. If the civilian defensive preparedness were at a high level and heavily involved the public, the public's reaction to a strategic warning to industry would probably not be a significant factor. If the general public were already taking protective actions, strategic warning to industry could provide further encouragement to protect themselves. If, on the other hand, the public were at a low level of civilian readiness, there would be no way to determine how the people would interpret such a warning or how they would react to it. Thus, considering the low level of civilian preparedness today, it does not appear feasible to give strategic warning to industry without first building up the public's general awareness of an impending crisis through the public media and then giving strategic warning or some other form of direction to the people at the same time that shutdown procedures are instituted by industry.

3. Lack of Formal Warning Channels. No formal communication channels presently exist from the federal government to industry over which a strategic warning could be disseminated. There are informal channels by which some industries keep attuned to a threat, but the concern generated by their knowledge of it is from the standpoint of how to prepare to meet the production demands that accompany a crisis rather than how to survive the attack which might be the end result of a crisis. In fact, the normal response to a crisis, i.e., to increase production to meet increasing needs for strategic materiel, is basically incompatible with the need to shut down production in order to enhance the probability of surviving the crisis.

At this time only a very general recommendation can result of this effort: a more comprehensive study should be made of key industries to determine more specifically the feasibility of providing strategic warning to industry, and the risks to industry and the surrounding communities of not responding to a warning to shut down versus the cost and consequent liabilities of a shutdown.

3.0 METHOD OF APPROACH

In the accomplishment of this task a survey was conducted of a small, but representative cross section of key industries that are essential to national survival, particularly in a postattack period. These were:

1. Steel
2. Food
3. Petroleum
4. Chemical
5. Banking

The selection of the particular company in each category was based on the fact that project personnel had previously made personal contact with the individuals in each of these areas. All of the industry contacts were responsible for emergency preparedness planning. The companies surveyed were:

1. Jones and Laughlin Steel Corporation, Pittsburgh, Pennsylvania.

2. General Foods Corporation, White Plains, New York.

3. Standard Oil Company of New Jersey, New York, New York (Humble Oil and Refining Company).[1]

4. American Cyanamid Company, Wayne, New Jersey.

5. Chase Manhattan Bank, New York, New York.

Representatives of each of these industries were interviewed for the purpose of obtaining the following kinds of information:

1. The time required for normal shutdown of the process that requires the longest shutdown time; the time required for shutdown of this process under accelerated, but orderly and safe conditions; and the time required for maximum-speed shutdown without regard to plant operability, but assuring personnel and area safety.

2. The physical and economic consequences to the plant of a maximum-speed shutdown; and the consequences to personnel and facilities in the area resulting from a failure to shut down. (Economic factors include shutdown and start-up costs, as well as capital, inventory production and contractual losses.)

---

1. The Standard Oil Company of New Jersey is a holding company of which the Humble Oil and Refining Company is a part. The emergency planning representative of the Standard Oil Company provided general information, but specific shutdown time and cost estimates were provided by the Humble Oil and Refining Company.

3. The degree to which shutdown could progress before the shutdown became common knowledge to plant personnel and people in the surrounding community; and the extent to which a skeleton crew could maintain operations in the plant in the event of an attack.

4. The type of information now available during a crisis to the industries studied and the source of that information.

In addition to the personal interviews, each representative was asked to provide this information in written form in response to a list of questions provided them. Though agreed upon willingly during the interview, the responses in terms of actually furnishing the data ranged from excellent to none at all. The information provided by the Humble Oil and Refining Company and Chase Manhattan Bank was detailed and complete. Jones and Laughlin Steel Corporation requested that it not be included in the study because it was not believed that any valid estimates of shutdown times could be made. No information was received from either the American Cyanamid Company or the General Foods Corporation.

Since not all of the industries queried responded in the detail requested, additional information was sought to provide a better basis for analysis and comparison.

Data were obtained from General Electric Company, Flight Propulsion Division, to augment the information received. In addition, the analysis draws upon information on rapid shutdown as a result of actual emergency experience. For this, the emergency shutdown of the following were examined:

1. Humble Oil and Refining Company, Baton Rouge Refinery, which occurred on 29 April 1960.

2. E. I. DuPont de Nemours and Company, Neoprene Plant, in Louisville, Kentucky, following an explosion on the morning of 25 August 1965.

Though the data available for this analysis are limited and do not reflect estimates of the emergency shutdown times of all of the five industries originally planned, sufficient material is on hand to allow a preliminary evaluation of the feasibility of shutdown, and the trade-off of shutdown as opposed to no shutdown.

4.0 DEFINITION OF INDUSTRIES

No two industries are exactly alike. Even though many companies in the same field produce like end products, e.g., automobiles, the production techniques, and the kinds of machinery and processes used are not always the same. In general, however, the functional makeup of companies in the same field is similar in that certain production phases must be reached. Going further,

many companies involved in the production of totally different items, e.g., petroleum and prime metals, are similar in that their operational makeup involves complex multistage production processes. With this in mind, then, it is possible to group the many different industries into categories according to the kind of operation in which they are involved.

In attempting to analyze the many aspects of an emergency shutdown (time requirements, resultant costs, consequences of not shutting down, etc.), it is necessary to differentiate between industries according to their type of operation. For this analysis, then, three general categories are chosen. These are: operational, discrete production, and continuous production.

1. Operational. The operational industry is a functional or service entity whose activities are concerned primarily with inventory manipulation and/or record processing. These activities do not involve complex processes which, if left unattended, could destroy themselves or their physical location. Banking and the insurance business fall into this category. To them, emergency shutdown is, for the most part, a matter of inventory and records security.

2. Discrete Production. The discrete production industry is concerned primarily with manufacturing. The activities here can involve a single or only a few production steps (making a funnel from a sheet of aluminum) or the assembly of finished parts into a particular item (an automobile production line), or can involve both machinery and limited processing (a jet engine factory makes parts, processes them by heat treating, and assembles them). To the discrete production industry, emergency shutdown is generally a matter of turning off machinery to avoid self destruction, and the stopping of any processes to eliminate fire and explosion hazard. While shutting down production can usually be accomplished quickly, the time required to stop a process is dependent upon its complexity. Some discrete production industries employ techniques that result in loss of materiel interrupted; thus, products using glue as a fastener generally involve spoilage if the operation is interrupted prior to the completion of a run.

3. Continuous Production. The continuous production industry is characterized by activities involving complex multistage production processes. As opposed to discrete production, the finished product here is derived by the changing of raw materials through processes involving many critical, sequential stages into an entirely new form and/or composition. Industries falling into this category are petroleum, steel, chemical, and so forth. The emergency shutdown of these industries is a complex, time-consuming, and costly operation often requiring as many critical and sequential steps as the process itself. It can involve not only turning off equipment, but cutting off raw materials feeding into the process, cooling down and depressurizing

heat treating ovens, and so forth. This is a critical series of steps which, if not taken, could result in damage to or destruction of the entire plant, and, in some cases, severe damage to the surrounding community.

5.0 SHUTDOWN FACTORS

5.1 SHUTDOWN TIMES

The minimal time required for a total nondestructive shutdown which would allow for complete abandonment of a plant without resulting damage to equipment or inventory, or any danger to the surrounding community, ranged from 20 minutes for a bank, to one and one half hours for the General Electric jet engine plant, to 20 hours for the Humble Oil Refinery. Though no particular limit was specified as to the duration of such a shutdown, the start-up of processing equipment is dependent upon the length of time it has been shut down. In the case of Chase Manhattan Bank, a totally operational entity, duration would have no effect upon start-up.

The minimal time required for a total shutdown without regard for equipment and process destruction or the physical consequences to the plant itself ranged from 20 minutes for a bank to four hours for an oil refinery. The discrete and continuous production industries consider such a shutdown extremely dangerous, however, in that the abandonment of production processes and equipment which have not been completely shutdown could result in fires and explosions which would affect not only the plant itself, but the surrounding community. In the most extreme case, the Humble Oil Refinery, it was learned that such a shutdown could be accomplished only if a skeleton crew remained to continue the depressurization of potentially hazardous equipment.

In the abandonment of an operational industry, such as Chase Manhattan Bank, without shutting down, the greatest hazard would be to the organization's inventory--the unguarded money and securities. Shutdown procedures are so clear and simple, however, and could be accomplished in such a short time that a no-shutdown situation is not even considered. On the other hand, the complete abandonment of operating production equipment and processes would almost surely result in major fires and explosions ranging from extreme damage to total plant destruction. The danger to the surrounding community would be very high, not only from explosions and fires on land, but fire spread through the sewer systems.

5.2 SHUTDOWN COSTS

The costs involved in a minimal time, total nondestructive shutdown depend, of course, on the kind and size of operation in question. For the operational industry, the task of shutting down merely involves the securing of inventory, and the shutdown and start-up costs would be negligible if anything at all.

In a discrete production industry, such as the General Electric jet engine plant, involved primarily in assembly with the only large scale processing units being heat treating furnaces, the shutdown, inventory loss, and start-up costs would be considered very low since, except for the furnaces which require time to cool down, the shutdown involves only the turning off of machinery. The biggest cost factor here would be resultant production losses should the shutdown be of an extended duration.

The cost concerns for a total nondestructive shutdown of a continuous production industry, such as the Humble Oil and Refining Plant, are a different matter. The shutdown costs alone are estimated at $25,000. Though no dollar figures could be approximated for inventory losses, they included such items as hydrocarbons to flare and slop, damaged catalysts and wasted chemicals, and some equipment damage such as plugged lines and tanks. The start-up costs after such a shutdown would approximate $100,000.

The above costs are all based upon estimates. The actual costs incurred in the emergency shutdown of the Humble Oil Company, Baton Rouge refinery on 29 April 1960, following a loss of steam and electric power, were in excess of $1,000,000. Though over half of this figure represents profit on lost production of critical products, the loss of raw materials, chemicals, and process catalysts cost $200,000. The remaining $300,000 is the dollar figure for mechanical damage, and the labor and materials for start-up. The duration of this shutdown was four days.[1]

It is interesting to note here that while the Humble Oil & Refining Company estimated that start-up costs after a typical refinery shutdown would be $100,000, in actual experience the figure ran to $300,000. This $300,000, of course, included equipment damage costs, but equipment damage as a result of the shutdown was considered light.

In the minimal time, total shutdown without regard for plant, equipment, and/or process destruction, costs could cover a wide range and are difficult to estimate. For Chase Manhattan Bank the costs would be negligible because again the concern is with inventory which can be quickly put away, and not with equipment or processes. No estimates were available on costs that would be incurred in a discrete production facility, but there is always a potential fire and explosion hazard, particularly in the case of incompletely shutdown furnaces.

---

1. F. P. Barrow, et al., Report on Emergency Shutdown - Baton Rouge, Refinery, April 29, 1960, ESSO Standard Division, Humble Oil & Refining Company, 15 November 1960. The four days referred to here was the time that elapsed from the moment the refinery ceased normal operations until normal operations were restored. Initial unit start-ups commenced 36 hours after the shutdown was complete, and continued on a unit-by-unit basis until normal operations were restored.

In a continuous production industry that is shut down without regard for equipment and process destruction, the costs involved would be considerable. Humble Oil and Refining Company estimates the losses could vary from $2,000,000 to one hundred times that much. In addition, assuming that fire and explosion effects are moderate, the damage to the surrounding community would amount to approximately $100,000.

A situation involving complete abandonment of a facility without shutting down would be very costly, could be disastrous, and would be an almost untenable alternative. In the case of a bank the cost could run to millions of dollars. Such a loss could result both from the stealing of unguarded cash and negotiable securities, and from fire due to the fact they had not been removed to the fireproof vaults. For the discrete production plant with even limited processing as well as the continuous production plant, the capital equipment loss would most probably be the entire plant.

5.3 PARTIAL SHUTDOWN

Partial shutdown and the continuance of limited operations with a skeleton crew is not considered practical for either the operations or discrete production industries because of the generally rapid response times to the shutdown order. It does, however, appear to be a desirable and most feasible alternative to the continuous production industry. The minimum time required, for instance, for a refinery to shift from full to limited operations on an orderly basis is approximately eight hours. Though the length of time required for shutdown is high and the shutdown and start-up costs are almost half those of a total nondestructive shutdown ($10,000 and $50,000 respectively), inventory losses are negligible, there would be no capital equipment losses, and start-up time would be cut considerably.

6.0 THE CONCEPT OF INDUSTRIAL WARNING

In attempting to determine whether to give strategic warning to industry to allow sufficient time to shut down, there are many factors to consider and many questions to answer. Why give industry strategic warning? Is warning industry separate from warning the general public a feasible concept? What are the consequences of giving such warning in terms of world tension and possible escalation of the crisis, of public reaction and possible chaos? What are the consequences of not giving it? These and many other questions must be answered before a valid determination can be made.

6.1 THE REQUIREMENT FOR INDUSTRIAL WARNING

Under present concepts, the allowable reaction time to a tactical warning--that is, warning given after a hostile attack has been detected--is, at best, between fifteen minutes and a half-hour in target areas. In reviewing the estimates of emergency shutdown times and the times associated with actual

emergency shutdowns that have occurred, it can be seen that a total nondestructive shutdown could not, in most cases, be accomplished within this time frame. In considering a total shutdown without regard for plant and equipment and/or process destruction, it is seen that even here the time constraints of a tactical warning are too stringent. The only alternative in a tactical situation seems to be no shutdown--abandon the industry and get the workers to shelter. But is this even an alternative? It has been pointed out that equipment and complex processes will, if left unattended, eventually destroy themselves and perhaps their entire surroundings. Aside from the banking business which could possibly respond to a tactical warning, the other critical industries will, for the most part, fall into the discrete or continuous production categories. If the effect of a hostile attack upon the nation's industrial capability is to be minimized--and it must if the nation's economy is to survive--then industrial facilities in areas not directly affected by the attack must not be allowed to add to the general destruction through their inability to terminate operations in a safe manner. Warning and shutdown procedures must be designed to maximize the survivability of the national industrial plant, recognizing that attack losses will be great enough without being further augmented by the self-destructive potential present in many processes.

6.2 FEASIBILITY OF INDUSTRIAL WARNING

Industry is the public. A warning to industry is a warning to the public. As such, public reaction must be taken into consideration, for the feasibility of providing industry strategic warning is greatly dependent upon how the public would respond.

In a threat situation, as a crisis develops and the tension increases, the public's concern about it can be expected to grow and their awareness of anything out of the ordinary to become acute. People seek information and direction, and without being told anything officially, will tend to accept any word, even rumor, as the truth and will react to it as they interpret it. (In such circumstances, unfortunately, the interpretation of the threat is very often that the danger is not personal or immediate.) If the public were at a high level of civilian readiness, that is, if they knew what they should be doing to protect themselves in the event of a hostile attack, this would not be a great problem, for if they began acting prematurely or even on wrong information, they would at least be going in the right direction.

In a previous chapter[1] it was pointed out that the release of official threat intelligence during a crisis comes to the public in the form of crisis information.

---

1. Chapter 2, "Decision to Warn."

How the public reacts to the receipt of this information depends upon the level of civilian readiness. If the civilian defensive preparedness is low, people seek direction as to what they should do, and often they react to official information as if they were being told what to do. How they interpret it and what actions they might take in such a situation are not always predictable.

Giving strategic warning to industry and not to the public when the civilian defensive posture is low could prove chaotic. In such a situation, where the people's knowledge of the crisis was due only to rumor, or at best, crisis information, a warning to shut down industry would compound in their minds the gravity of the threat, and their reactions would be swifter and more erratic. The word of a shutdown would pass very quickly--to the families of the workers, their neighbors, the community--and each retelling would be flavored by inevitable rumor. The press would pick it up and in a matter of hours the news would be all over the nation. There could be complete loss of control for, without direction, there would be no way to tell how the public might react.

Some industries say that a major shutdown could be started by a few key people, and that all of the workers would not have to be told until it was underway. This might be true, but the sensitivity of people in a tense crisis situation make it questionable that it could go very far before the workers knew that something unusual was happening.

Considering the general low level of civilian preparedness which prevails today, it does not appear feasible to give strategic warning to industry without first conditioning the people through the management of crisis information so that they will react in the desired way, or actually directing them to action through public strategic warning. Giving industrial strategic warning in this way would have the positive side effect of giving more credence to managed crisis information or bolstering a public strategic warning, and would be a means of demonstrating the seriousness of the nation's intentions. On the negative side, however, such an action could be considered hostile and could rapidly escalate the crisis or even preempt an enemy attack.

In addition to the negative aspects of industrial strategic warning without some form of public strategic warning, there is also the problem that no formal communications channels presently exist from the federal government to industry, either classified or unclassified, over which such a warning could be disseminated. Informal channels could probably be established in a relatively short time over which warning could be given to a few of a selected group of industries; but, any attempt to set up communications over which either a general industrial warning or one even to just those elements of industry requiring the longest shutdown lead time, i.e., petroleum, chemical, etc., would be an almost impossible task in anything but a prohibitively long time period.

Some industries have warning systems, but these have generally been set up independently on an industry-by-industry basis and are tied to the civil defense organization only at the local level. For instance, Chase Manhattan Bank has a bell and light system over which they claim they would receive warning direct from NORAD.

Since there is no voice capability tied to the system, other than a separate radio link with the local police for authentication, this is really only an alerting device. From the reference "direct from NORAD" and the fact that the alert signal is authenticated by the police department, it appears that this system is a tailored extension of NAWAS. Though no more definite information was available, discussions with the Chase Manhattan Bank representative revealed that the system was designed to provide tactical alerting, not strategic warning.

There are informal channels through which some industries keep attuned to crisis situations, but these are more of the intelligence variety as opposed to warning channels. The Standard Oil Company of New Jersey, for example, learns much about how and to where the nation plans to deploy its forces in a crises by the kinds of fuel that are ordered and where these fuel orders are to be sent.

From this it measures the gravity of the situation. It was found, however, that any concern that is generated by the threat is usually from the standpoint of how profits might be affected, not survival.

6.3 COST CONSIDERATIONS

From the standpoint of industrial survival, cost is not a consideration. For the economy to recover from a nuclear attack, industry must survive at all costs. But in determining how and when industrial strategic warning might be given, there are many peripheral costs which must be considered, for they will greatly influence any decision.

In a total shutdown affording maximum protection for equipment, inventory, and the physical plant, production profit losses were considered the largest single cost by all industrial representatives interviewed. In reviewing the actual costs incurred in the emergency shutdown of the Humble Oil Company, Baton Rouge Refinery, it is seen that the most significant single cost was the loss of profit due to the total halt in production. This loss was figured at $500,000, half of the total shutdown cost, and was representative of a shutdown of only four days. The second most significant estimated cost is start-up after shutdown and mechanical damage to equipment as a consequence of the shutdown. In the case of the Baton Rouge Refinery again, this accounted for approximately $300,000, or about one-third of the total costs incurred. The remaining costs are accounted for in inventory losses (this factor is most predominant in the continous production plant where inventory is primarily

chemicals, processing catalysts, etc.) and salaries which continue to be paid while the plant is shut down. During the Baton Rouge refinery shutdown this latter amount was in excess of $200,000.

An emergency shutdown is not inexpensive. Consider that the shutdown of a single oil refinery, and for only a four day period, cost in excess of one million dollars. Now multiply this figure by all of the refineries and plants in the entire petroleum industry and dollar losses of many millions results. Though shutdown cost figures were not available for other industries, particularly in the continuous production category, it is not difficult to imagine hood of a billion dollars. This figure would take into consideration actual shutdown costs, inventory and capital equipment losses, salaries and production profit losses for a minimal time shutdown, and actual start-up costs. For a total shutdown over an extended period, additional production profit losses and salary expenses would have to be added, plus any costs as a result of equipment damage.

If the nation actually declared a strategic warning and industry were able to shut down before the country was hit by nuclear attack, then these costs, as great as they might be, would be of little consequence in terms of industrial survival. But if a strategic warning were declared and total industrial shutdown followed, but the attack did not materialize, of what consequence then would these costs be? Exactly where would the liability for a false alarm fall? Of what consequence to the national economy would a total demobilization of industry be?

Many industries have in their disaster plans the provision to continue paying salaries to their employees in the event of emergency shutdown and/or plant destruction. They have even gone so far as to establish temporary payroll distribution centers where they store predrawn and signed payroll checks. This has been done because the industries truly believe that their personnel are the key to ultimate survival, and the costs involved are necessary. In a false alarm situation, however, where salaries would still have to be paid, but the reason for shutdown was not valid, what then would be the attitude of industry? Who then should foot the bill for even this one "unnecessary" expense?

Several of the major industries queried in this study indicated that all of their production contracts carried a standard caveat stating that in the event of a shutdown as a result of natural or man-made disaster, contractual commitments, such as delivery times, would not be binding. Thus, in an actual emergency shutdown this would not be a financial problem from this standpoint. However, all of the industrial representatives interviewed did not believe that this caveat would be applicable in a false alarm shutdown, and that they would be financially liable for failure to meet any contractual commitments. To go one step further, what about the manufacturers that depend upon major industry as a source of supply? What about their liability when they cannot fulfill a commitment.

These are but a few of the cost considerations of the consequences of a false alarm. What about start-up costs, inventory losses, production profit and equipment losses? The question again: Who would pay these bills?

6.4 ADDITIONAL CONSIDERATIONS

The consequences of a false alarm industrial strategic warning would probably be most obvious from an economic standpoint, but there are other factors which would weigh heavily upon any decision to give it. The effect upon the international situation would be great, particularly if a strategic warning were based upon a false evaluation of the threat, and the warning precipitated enemy action. A false alarm would greatly undermine public faith in the credibility of warning. The effect upon the morale of the public--the problems of what to do with millions of people released from work until industry could return to normal operations could result in complete loss of control in the situation.

The question of industrial strategic warning presents the policy makers and the decision makers with a dilemma. A decision to give the warning would be based upon the belief that a hostile attack was imminent. Not to give it in the face of such a threat could be suicide should the attack materialize; but, to give it and have the warning turn out to be a false alarm, could spell disaster of a magnitude not yet fully contemplated.

CHAPTER FIVE

RELIABILITY OF A GENERALIZED WARNING SYSTEM

1.0 INTRODUCTION

The purpose of this chapter is to provide a theoretical background for the establishment of reliability requirements for warning systems still in the conceptual stage.[1] Also presented is the rationale for optimal system testing, given the reliability functions for the system. The approach is to provide "building blocks," from which any warning system can be modeled for reliability purposes. No consideration is given to the timeliness of warning or the individual's response to a warning. All results are couched in terms of the number of components effected by either the receipt of a false warning, or the failure to receive a valid warning.

This chapter is addressed to a dual audience, i.e., those knowledgeable in reliability theory and those who are not. Therefore, the theory behind the methodology used to analyze systems is developed in detail for the noninitiates. The theoretical development has also been necessitated by the fact that little work has been done in the theory of components that can fail in two modes; this two-mode failure is developed throughout the paper.

The analysis performed relates to the real problems of the system designer and the system operator. It is anticipated that the method of analysis will be applied by System Development Corporation to its future efforts in developing the Decision Information Distribution System (DIDS) and the Radio Warning System. It is available for use by personnel in and contractors to the Office of Civil Defense for the evaluation and/or improvement of existing systems such as the National Warning System (NAWAS) and the Washington Area Warning System (WAWAS). To facilitate the application of the method of reliability analysis described in this chapter to future problems, worksheets and complete computational instructions are developed and described.

2.0 CONCLUSIONS AND RECOMMENDATIONS

This study shows that from the basic reliability data available (or assumed) on the components of a warning system, it is possible to develop, in a statistical sense, the operating characteristics of that system in terms of the components

---

1. This chapter supersedes Reliability and Warning Systems, which was originally published as TM-L-1960/070/00, dated 14 January 1966.

effected by false alarm and no alarm failures, the expected number of false alarm and no alarm situations, and the expected durations of these situations. Although these factors do not, of course, tell all about system effectiveness, they do give an indication as to how well a system will satisfy the needs of the public and the warning agency. The development of the concepts in this study are based on the exponential assumption and are not necessarily valid for other failure distributions. However, all of the concepts can be redefined for other failure distributions by use of the methodology herein contained.

In the area of work to be done in reliability of warning systems, the establishment of rigid standards is mandatory. Just what is an acceptable number of false alarm or no alarm failures per year? What is the minimum requirement for system performance? What is the maximum number of hours of downtime per year per terminal warning device acceptable for adequate warning? These questions are really nothing more than variations of the fundamental question: what percentage of the population may be put at risk because of either a false alarm or a no alarm failure? This question and its derivations must be answered even by command decision, if necessary. Theoretical studies cannot evaluate human beings in mathematical terms.

A second area requiring exploration is the relationship between cost effectiveness and reliability. This would mainly be a study of sophisticated components vs. cheap, redundant components in their overall effect on system performance. This is a standard reliability procedure and should require no more than a literature search with some development to take into account the two modes of failure.

It has been pointed out that the extension of the methodology developed in this study can be extended to other failure models. If a more sophisticated model is needed to evaluate specific warning systems, and if the necessary data on failure distributions is available for these systems, the model should be extended and computerized for a finer grained analysis of such systems.

By computerization, and Monte Carlo techniques, it is possible to gather distributional data rather than averages as in this study. Rather than assume a symmetrical system as examplified in the hypothetical National Warning Dissemination Study, it is possible to distribute realistically the various warning dissemination levels with respect to the population, and even more importantly, to adjust the various failure rates to correspond, for instance, to the seasonal variations in noise levels in radio links or to the population distribution with respect to day and night situations. With these adjustments, the model could then be run and reasonable distributions derived for the percentage of population in jeopardy for various situations.

In light of the above conclusions, the following recommendations are made:

1. Required Reliability. Define the required reliability that a warning system must possess before it is acceptable for OCD warning purposes.

2. Cost Effectiveness. Explore the relationship between cost effectiveness and reliability for warning systems.

3. Computer Model. Computerize the developed model to determine the effects of population mobility, and of different failure modes of the warning system, etc., on the efficacy of the warning system.

3.0 CONCEPTS AND DEFINITIONS

3.1 DEFINITIONS

A warning system is defined as a collection of entitites capable of disseminating warning from the originator to the ultimate recipient of the warning. A subsystem is any clearly identifiable portion of the system capable of receiving and/or disseminating further the warning message. A warning device is a special subsystem used to disseminate the warning to the ultimate recipient.

A component is a self contained, independently operable portion of a system whose functions are described in terms of the overall system mission. In terms of warning systems, then, a siren is a component, while the motor that drives the siren rotor is not; a radio transmitter is a component, while its power supply is not. Thus a component of a warning system is the smallest assemblage of elements that is capable of disseminating warning.

3.2 RELIABILITY

For the purposes of this study, reliability is defined as the measure of system (or subsystem) availability and response, i.e., the probability that the system (or subsystem) will be able to perform its assigned function when called upon to do so, and not otherwise. By knowing the population distribution with respect to the warning devices, it is then possible to determine, in a statistical sense, the proportion of the population that will be placed in jeopardy because of lack of warning or false warning.

3.3 FALSE ALARM FAILURES AND NO ALARM FAILURES

The above definition of reliability recognizes both false alarm failures and no alarm failures as system failures. Inclusion of both types of failures in the definition of reliability is necessary when discussing the overall reliability of a system or component, for, in the case of either type of failure,

the system or component is not performing as it should. In a warning system, however, these two types of failures present distinctly different hazards to the population. In the false alarm situation, there can be a complete disruption of community affairs and a tendency, if such false alarms are comparatively frequent, to undermine the public's faith in the warning system. In the no alarm situation, the hazard is obvious. For these reasons, then, the two situations are separated in the development of the model.

3.4 CONSTRAINTS

In order to prevent confusion in the latter portion of this study, the following constraints apply:

1. The study is restricted to maintained systems operating in a steady state, i.e., operating long enough that the failures are random in nature and not the result of breaking in or turning on the systems.

2. No attempt is made to determine the effects of sabotage on any portion of the system.

3.5 THE WARNING SYSTEM CONFIGURATION

The general system configuration to be studied assumes the existence of one or more originating points (for purposes of this study, referred to as Central Warning Points or CWPs). The CWPs disseminate disaster information to intermediate centers (in this study called Repeater Warning Points or RWPs), which, in turn, disseminate the information to the public or to local warning facilities (called Terminal Warning Points or TWPs). This procedure may be manual or automatic, or a combination of both. It is also assumed that the generalized system is a fanout system without loops, i.e., the system is similar in overall structure and function to that existing in the current civil defense warning system or to that proposed for the National Emergency Alarm Repeater (NEAR) System or the Radio Warning System. The generalized system is illustrated in Figure 5-1.

The numbers in the lower right hand corner of each box identify the level of that box. They are numbered serially from the originator to the recipient and signify that each box with the same number is identical in nature and function.

4.0 THE EXPONENTIAL ASSUMPTION

The exponential assumption asserts that, in general, equipments exhibit a probability of failure according to the function[1]

1. See Section 5.2.

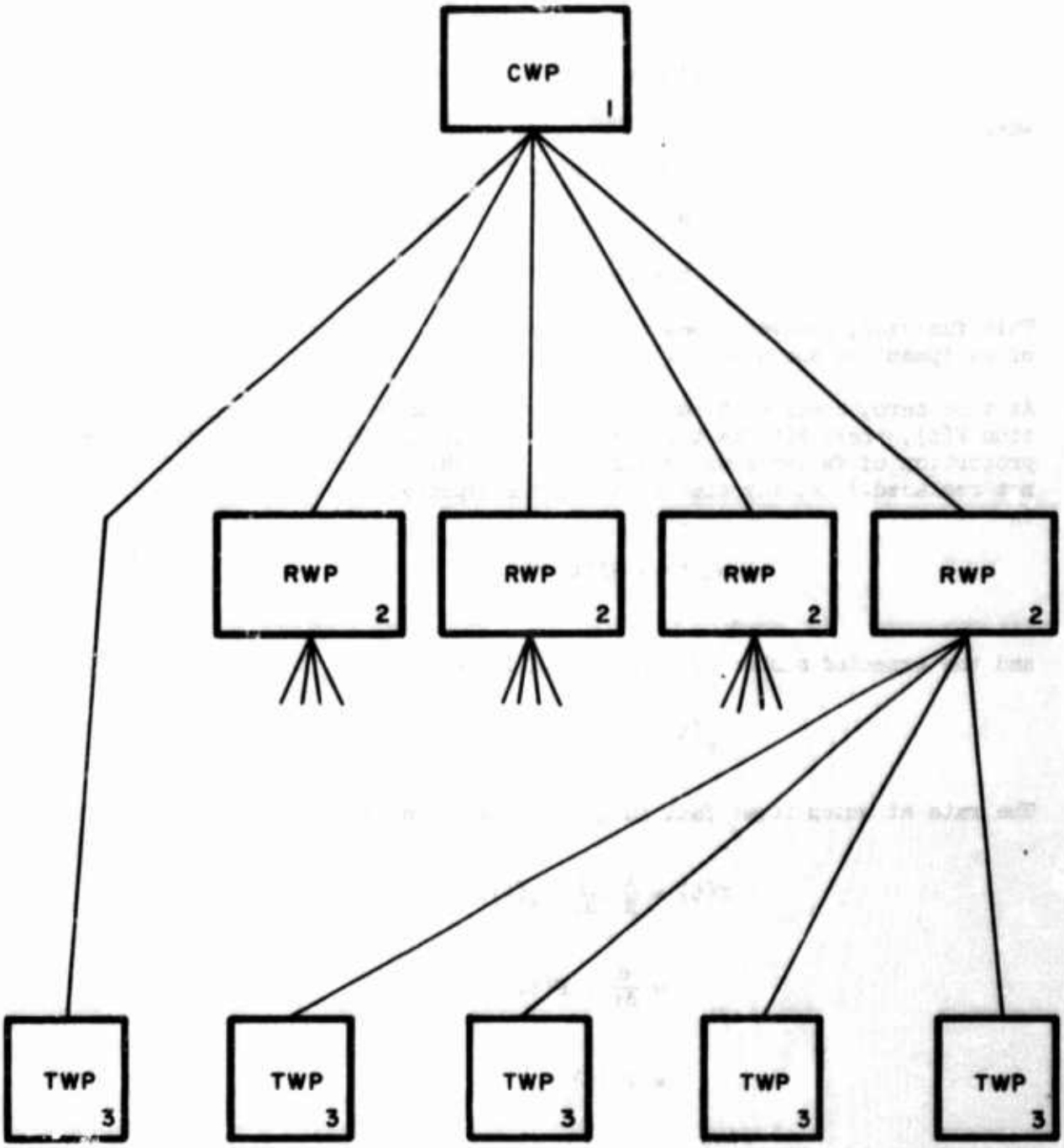


Figure 5-1. Typical Fanout Network (Note: Each RWP has the same number of TWPs attached. They have been omitted for clarity).

$$r(t) = e^{-\frac{t}{\theta}}$$

where

$r(t)$ = the probability of survival to time t

θ = the mean time to failure, and

t = the elapsed time since the beginning of operation.

This function, however, does not correspond to the real behavior of many items of equipment as shown below.

At time zero, consider N identical items with an arbitrary failure distribution F(t), where F(t) is the cumulative distribution function giving the total proportion of failures up to time t. (For this discussion, failed items are not replaced.) At any time t, then, the expected number of failures, $n_f(t)$, is

$$n_f(t) = NF(t)$$

and the expected number of items still functioning, $n_s(t)$, is

$$n_s(t) = N[1-F(t)]$$

The rate at which items fail in general is given by

$$f(t) = \frac{1}{N} \cdot \frac{d}{dt}[n_f(t)]$$

$$= \frac{d}{dt} \cdot F(t)$$

$$= F'(t)$$

The conditional failure rate, however, given a number or items that have survived to time t, is the rate at which those items fail at time t. Therefore, the conditional rate at which items fail at time t, provided that they have survived up to time t, is

$$h(t) = \frac{\frac{d}{dt}[n_f(t)]}{n_s(t)}$$

$$= \frac{f(t)}{1-F(t)}$$

The function h(t) is called the hazard function. Now if F(t) is the probability an item has failed some time prior to t, then 1-F(t)=r(t), is the probability of survival to time t. Substituting

$$r(t) = e^{-\frac{t}{\theta}}$$

then

$$f(t) = F'(t)$$

$$= \frac{1}{\theta} e^{-\frac{t}{\theta}}$$

therefore

$$h(t) = \frac{\frac{1}{\theta} e^{-\frac{t}{\theta}}}{e^{-\frac{t}{\theta}}}$$

$$= \frac{1}{\theta}$$

Since the hazard function, h(t), is independent of time, the exponential assumption does not allow for "wearout" of items, i.e., the probability of the failure of an item is independent of the length of time that the item has been used.

Despite the above lack of realism in the exponential assumption, it is widely used in reliability work because it does give good approximations of observed failures in steady state operations of equipments. Note, though, that it is generally inapplicable in non steady state operations, such as break in periods, etc. Its simplicity also allows the development of the underlying principles of reliability that would be otherwise lost in a mountain of mathematics; this

characteristic of the exponential distribution is particularly valuable in a developmental study such as this. For these reasons, then, the exponential assumption is used throughout the study with the understanding that, in reality, any other suitable probability distribution can be used with the methodology developed herein.

5.0 THE BASIC COMPONENT RELIABILITY MODEL[1]

5.1 STATE PROBABILITIES

This study is specifically concerned with investigating a generalized component with the states of operation (or nonoperation) given in Table 5-1.

Table 5-1. States of Operation

State	Meaning
P_0	The component is operating in a satisfactory manner.
P_1	False alarm state; the component is operating when it should not be.
P_2	No alarm state; the component is not operating when it should be.

In order to discuss the transition probabilities from one state to another, a transition matrix P is constructed. Given that a is the rate of false alarm failures per unit time for a component (or a system), and b is the rate of no alarm failures, then the probability of the equipment remaining in operation (state P_0) during the time period from t to t+dt is 1-(a+b)dt, the probability of failing on (state P_1) is adt, and the probability of failing off (state P_2) is bdt. If the rate of repair of failed equipment is m, then

1. For further information on this subject, see G. H. Sandler, System Reliability Engineering, Prentice-Hall, Co., Englewood Cliffs, New Jersey, 1963, from which much of this material is derived.

the probability that a piece of equipment already failed into either state P_1 or P_2 will return to the operational state P_0 in the period from t to t+dt is mdt. The transition matrix shows the probabilities p_{ij} of going from state P_i at time t to state P_j at time t+dt where i denotes the row number of the matrix and j deontes the column number.

$P(t) =$

	P_0	P_1	P_2
P_0	1-(a+b)dt	adt	bdt
P_1	mdt	1-mdt	0
P_2	mdt	0	1-mdt

To make these transition probabilities meaningful, in a reliability sense, to this examination, the matrix must be converted into a series of equations such that the probability of being in a given state is given as a function to time, t, from the beginning of component operation. The procedure is as follows:[1] the probability that the component is in state P_0 at time t+dt is the sum of three probabilities that express the three mutually exclusive ways in which the equipment can arrive in that state: (1) the equipment was already in state P_0 at time t with probability $P_0(t)$ and remained in that state until t+dt with probability 1-(a+b)dt; (2) it was in state P_1 at time t with probability $P_1(t)$ and returned to state P_0 (i.e., was repaired) at time t+dt with probability mdt; or (3) it was in state P_2 at time t with probability $P_2(t)$ and returned to state P_0 at time t+dt, also with probability mdt. The probability that the component was in state i at time t and moved to state j at time t+dt is expressed as the product of the separate probabilities of (1) being in state i at time t and (2) of moving to state j at time t+dt. There-

1. Emanuel Parzen, Stochastic Processes, Holden-Day, Inc., San Francisco, California, 1964, pp. 276 ff.

fore the probability of being in state P_0 at time t+dt can be expressed as follows:

$$(1) \qquad P_0(t+dt) = P_0(t)[1-(a+b)dt] + P_1(t)mdt + P_2(t)mdt$$

Similarly it can be shown that the probabilities of being in states P_1 or P_2 at time t+dt can be expressed as:[1]

$$(2) \qquad P_1(t+dt) = P_0(t)adt + P_1(t)(1-mdt)$$

$$(3) \qquad P_2(t+dt) = P_0(t)bdt + P_2(t)(1-mdt)$$

In order to remove the variable t+dt from equations (1)-(3), the definition of the differential of a function is employed

$$P_i'(t) = \frac{P_i(t+dt) - P_i(t)}{dt}$$

where the prime indicates the differential with respect to time. Mathematical manipulations result in the following three simultaneous differential equations:

$$(4) \qquad P_0'(t) = -(a+b)P_0(t) + mP_1(t) + mP_2(t)$$

$$(5) \qquad P_1(t) = aP_0(t) - mP_1(t)$$

$$(6) \qquad P_2'(t) = bP_0(t) - mP_2(t)$$

Solving these simultaneous differential equations assuming that the component was operating at t=0, it is found that

$$P_0(t) = \frac{m}{a+b+m} + \frac{a+b}{a+b+m} e^{-(a+b+m)t}$$

---

1. Note that it is assumed in this example that equipment cannot move from one of the failed states to the other.

$$P_1(t) = \frac{a}{a+b+m}\left[1-e^{-(a+b+m)t}\right]$$

$$P_2(t) = \frac{b}{a+b+m}\left[1-e^{-(a+b+m)t}\right]$$

These equations now give us the probabilities of the components being in any given state at any given time t. Since this study is concerned with steady state operation (i.e., t approaches infinity), the equations reduce to

(7) $$P_0(\infty) = P_0 = \frac{m}{a+b+m}$$

(8) $$P_1(\infty) = P_1 = \frac{a}{a+b+m}$$

(9) $$P_2(\infty) = P_2 = \frac{b}{a+b+m}$$

5.2 COMPONENT RELIABILITY AND FAILURE RATES

Equations (7)-(9) give the probability the component is in a given state at a given time, but tells nothing of the history of states it has been in up to that time. However, the equations that produce the mean time to first failure (MTTFF) of the component, as well as the number and distribution of failures are derived below.

$P(t) =$

	P_0	P_1	P_2
P_0	1-(a+b)dt	adt	bdt
P_1	0	1	0
P_2	0	0	1

The corresponding differential equations are

$$P_0'(t) = -(a+b)P_0(t)$$

$$P_1'(t) = aP_0(t)$$

$$P_2'(t) = bP_0(t)$$

Recognizing that the reliability probability, r(t), is the modified $P_0(t)$, the first equation need only be solved. Thus

$$r(t) = P_0(t) = e^{-(a+b)t}$$

The latter expression is the probability that either a false alarm or a no alarm situation will not exist in the component from time 0 to t. The failure distribution, F(t), must, therefore, be

$$F(t) = 1-r(t)$$

$$= 1-e^{-(a+b)t}$$

F(t) gives the probability that the component has already failed before time t. To determine the MTTFF, F(t) is differentiated with respect to t to get the instantaneous probability of failing at time t; this is multiplied by t, and then integrated to obtain the mean, from t=0 to t=∞. Thus

$$(\text{MTTFF}) = \int_0^\infty \frac{dF(t)}{dt} t\,dt$$

$$= \int_0^\infty t(a+b)e^{-(a+b)t}\,dt$$

$$= \frac{1}{a+b}$$

By a similar argument, it can be shown that the mean time to failure for false alarm, denoted (MTTFF(1)), and for no alarm, denoted (MTTFF(2)), is

$$[\text{MTTFF}(1)] = \frac{1}{a}$$

$$[\text{MTTFF}(2)] = \frac{1}{b}$$

To determine the mean time to repair (MTTR), the procedure is as above, but P_0 is treated as the absorbing state and the initial state is either P_1 or P_2, since both have been assumed to have the same repair distribution. This then gives G(t), the repair distribution as

$$G(t) = 1\text{-}e^{-mt}$$

$$\frac{d}{dt} G(t) = me^{-mt}$$

and, thus as before

$$\text{MTTR} = \int_0^\infty t \frac{d}{dt} G(t)\,dt$$

$$= \int_0^\infty tme^{-mt}\,dt$$

$$= \frac{1}{m}$$

What has been presented thus far applies to a component only during its initial operating phase before its first failure. The operating characteristic of the component during a given time period 0 to T, in which it might fail and be repaired several times, can be explored through the use of renewal theory.[1] Renewal theory provides the expected number of repairs and/or replacements that must be made during the period under consideration.

1. Richard Bellman, A Survey of the Mathematical Theory of Time-Lag, Retarded Control, and Hereditary Processes, The RAND Corp., R-256, 1 March 1954; Parzen, op. cit., pp. 160 ff.

Let $u_{00}(t)$ be the expected number of times the component returns to an operating state, assuming that it was operational at t=0, and $u_{10}(t)$, the expected number of returns to an operating state given that the component was initially failed. Then, the equation for the expected number of repairs $u_{00}(t)$ can be found from the two simultaneous integral convolution equations.

$$u_{00}(t) = \int_0^t u_{10}(t-x)dF(x)$$

$$u_{10}(t) = \int_0^t [1+u_{00}(t-x)]dG(x)$$

The solution to these equations gives[1]

$$u_{00}(t) = \frac{(a+b)mt}{a+b+m} + \frac{(a+b)m[e^{-(a+b+m)t}-1]}{(a+b+m)^2}$$

or, when t is large

$$u_{00}(t) = \frac{(a+b)mt}{a+b+m} \tag{10}$$

Equation (10) indicates, then, that in a certain time period T, there are $\frac{(a+b)mT}{(a+b+m)}$ equipment failures of either a false alarm or a no alarm type. In order to determine how many of each type can be expected, the following reasoning applies. Given the probabilities a and b of two mutually exclusive events A and B, and knowing that one of them has occurred, then the probability that it was A is

$$P(A) = \frac{a}{a+b}$$

and that it was B

$$P(B) = \frac{b}{a+b}$$

---

1. Sandler, op. cit., pp. 118-119.

Given N occurrences of A and B, the expected number of As, E(A), is

$$E(A) = N\,P(A) = \frac{Na}{a+b}$$

and of Bs

$$E(B) = N\,P(B) = \frac{Nb}{a+b}$$

In the example being discussed, N is given by the expression for $u_{00}(t)$; a is the probability of a false alarm failure; and b is the probability of a no alarm failure. Therefore, the expected number of false alarms in a time period T is

$$E(1) = \frac{a}{a+b}\,u_{00}(T)$$

$$E(1) = \frac{amT}{a+b+m} \qquad (11)$$

The expected number of no alarms is

$$E(2) = \frac{b}{a+b}\,u_{00}(T)$$

$$E(2) = \frac{bmT}{a+b+m} \qquad (12)$$

5.3 OPTIMAL COMPONENT TESTING

The purpose of component testing is to maximize the number of components available. There are three distinct cases that must be considered. In two cases, checkout time is not considered as downtime, i.e., even though the component is being tested, it is available to perform its assigned task; in one of the no-downtime cases, continuous monitoring of the component is feasible, while in the other continuous monitoring is not feasible. In the third case, checkout time is considered as downtime, i.e., the component cannot perform its assigned task while it is being tested. A no-downtime situation arises, for instance, in the case of a voice or hard-copy system, in which the test message can be made sufficiently different from the warning

message to be readily identified as a test message and an interrupt capability exists. A downtime situation arises, for instance, in the case of a siren warning system, since the warning signal and the full test signal are sufficiently similar that an interrupt signal does not really exist. Thus three cases are treated separately: (1) no downtime, continuous checkout; (2) no downtime, discrete checkout; and (3) checkout with downtime.

Before developing the necessary formulas, it is necessary to point out that this discussion is limited to a large assemblage of similar components that are operating in a steady state condition, i.e., a sufficiently long time period so that there exists a wide distribution of ages in the components. It is only in this way that the optimal checkout interval, T_c, can be determined in a statistical manner.

In the first case, where checkout time is not downtime, an optimal checkout period does not exist. With continuous checkout, it can be shown from queueing theory that the average proportion of components, $H(0)$, in repair is

$$H(0) = \frac{a+b}{m}$$

Any discrete checkout scheme, in which checkout is not continuous, will have a proportion of components failed or in repair greater than $H(0)$. The checkout policy in this case is to decide in advance the average maximum proportion, $H(T)$, of components that can be inoperative for any reason. Note that two failure processes are being dealt with. Those components that fail in an on condition will be noted and repaired without delay, but those components that fail in an off condition must be tested before the failure can be noted and repairs made. Thus the first type of failure produces a constant proportion of components, a/m, that are in repair. The second type of failure produces failed but undetected failures at the rate of bt, where t is measured from the last check. When a check is made at time intervals of length T_c, the number of components out of service is given by the expression $a/m+bT_c$. During the repair interval, $1/m$, b/m more components will fail. Thus, by summing these to determine the total maximum number of components out of service, it is found that

$$H(T_c) = \frac{a+b}{m} + bT_c$$

$$= H(0)+bT_c$$

The testing interval would then be

$$T_c = \frac{H(T_c)-H(0)}{b}$$

(Note that, for instance, the actual rate of failing in an off condition is

$$F_2(t) = 1-e^{-bt}$$

However, the approximation

$$F_2(t) \approx bt$$

derived from the approximation

$$e^{-x} \approx 1-x$$

is sufficiently accurate for the purpose of this study as long as $bt < 0.25$.)

When checkout time is considered as downtime, there indeed exists an optimal checkout interval. The measure of effectiveness to be used here will be to minimize the average number of inoperative components over the test cycle T_c and thus maximize the average component availability. The function $H_1(T)$ is defined as

$$H_1(T) = t_c + \int_0^T H(t-t_c)dt$$

where t_c is the time necessary to check the system out. The next step is to find a $T=T_c$ such that $H_1(T_c)/T_c$ is minimum for a given t_c. Note that, since t_c is considered downtime in this case, all components are unavailable during checkout. Again using the approximation for failure rates, and eliminating duplicate downtimes because of the failures occurring during the checkout interval, it is found that

$$H_1(1) = \frac{1}{2}b(T-t_c)^2 + t_c + T\left(\frac{a+b}{r}\right) - \frac{atc}{m}$$

$$\frac{H_1(T)}{T} = \frac{bt}{2} - bt_c + \frac{bt_c^2}{2T} + \frac{t_c}{T} + \frac{a+b}{m} - \frac{at_c}{mT}$$

Differentiating this with respect to T, setting the result equal to zero, and solving for T ($=T_c$), it is found that

$$T_c = \sqrt{\frac{t_c(2+bt_c-2(a/m)}{b}}$$

For reasonably small failure rates this becomes

$$T_c = \sqrt{\frac{2t_c}{b}} \qquad (13)$$

Note as t_c approaches zero, T_c does also, and the same situation develops as in the case of no-downtime checkout.

In comparing the average number of unavailable components over the same period T_c for the two concepts of checkout, it is obvious that the average unavailability is greater for the downtime checkout than for checkout without downtime. The average component unavailabilities for the three cases (no downtime, continuous checkout; no downtime, discrete checkout; checkout with downtime) are as follows: (The approximately equal signs are used because of the linear approximation of e^x.)

No downtime, continuous checkout:

$$A(0) \approx H(0) \qquad (14)$$

No downtime, discrete checkout:

$$A(T_c) \approx H(0) + \frac{bT_c}{2} \tag{15}$$

Checkout with downtime:

$$A_1(T_c) \approx H(0) + \frac{b(T_c - t_c)^2}{2} + \frac{t_c}{T_c}\left(1 - \frac{a}{m}\right) \tag{16}$$

Examining these three equations, it is obvious the continuous checkout is the best policy if failures in the off state can be detected, or if the equipment is such that repair only upon failure is a feasible policy from a cost viewpoint.

To summarize, component testing maximizes the availability of that component in some statistical sense, but also has a profound effect on the overall availability of the component. This side effect is used in Section 5.4 to determine an overall criterion for component performance.

5.4 ULTIMATE MEASURE OF COMPONENT PERFORMANCE

Returning to the original definition of reliability in Section 3.1, above, it should be obvious now that what is really sought is a measure that gives the probability that a component will perform its function in a warning system when called upon to do so. It must not only be available, say, at time t, but it must not fail in the no alarm state during the warning period t to t+x, where x is the duration of warning. Therefore, a suitable measure of component performance, S, for a single warning is

$$S = [1-A(.)]\ [1-\int_t^{t+x} P_2(y)dy]$$

Since what is dealt with here is steady state operation,

$$S = [1-A(.)]\ [1-P_2(\infty)]$$

$$= [1-A(.)]\left(\frac{a+m}{a+b+m}\right)$$

where A(.) is the appropriate availability function (derived in Section 4.3) and the parenthetical part, (a+m)/(a+b+m), is the probability that the component will not fail off during the warning period of duration x. This assumes that the warning is given only once. However, if warning is required more than once, then $S^{(n)} = S^n$, where n is the required number of individual repetition, $S^{(n)}$ is the measure of component operation for n operations of the component, and the time interval between the start of warning is greater than x, i.e.. the warnings are distinct and do not run together. In light of the above derivation, then, $S^{(n)}$ (n = 1,...) will be used as the performance criteria for components in evaluating overall system performance.

5.5 DETERMINATION OF REQUIRED COMPONENT RELIABILITY

Frequently, only the desired system reliability is given in system specifications, and it is necessary to allocate required reliabilities among the various components involved. Examples can be found in the 416L (SAGE) requirements, which dictated that the system unavailability should not exceed four hours per year, or in the 477L (NUDETS) system, which specified a 90 percent availability. In neither case did the reliability requirements go beyond these figures in amplifying the reliability requirements for subsystems or components. System designers cannot, however, trust to luck hoping that the requirement can be met. Therefore, allocation of system reliability requirements is a legitimate area of investigation in this study. Therefore, two cases are considered: the first that all components are of equal importance; and the second, that all components are not of equal importance and that their relative importance can be estimated.

Recalling that the probability of the simultaneous occurrence of independent events is the product of the probabilities of their individual occurrences, this fact can be applied to determine the reliabilities of various components connected in series. Thus, if all the components have equal importance, the required reliability of the i^{th} component is

$$S_i = S^{\frac{1}{n}} \tag{18}$$

where

S = required system reliability

S_i = required component reliability, and

n = number of components in the series

If the relative importance of each component, E_i, has been established, then the problem is to find a number k_i such that

$$(19) \quad \begin{cases} S_i = S^{k_i} \\ k_i = < 1 \\ \Sigma k_i = 1 \end{cases}$$

After some elaborate manipulation, it can be concluded that

$$(20) \quad k_i = \frac{1}{mnE_i}$$

where m is a normalizing factor and is found by the relation

$$(21) \quad m = \frac{1}{n} \Sigma \frac{1}{E_i}$$

Note that the only restriction on E_i is that it be greater than zero. In the case where there exist parallel paths, i.e., the configuration is redundant, the duplicate components are lumped together for the initial allocation and are treated as one component. Then, to determine required reliability of each component that has been lumped, the procedure is exactly as above, but instead of using S and S_i in the computations, Q=1-S is substituted for S, and Q_i=1-S_i for S_i. This method is applicable only if the system does not require both components for satisfactory operation, i.e., the components in question are truly redundant.

6.0 COMBINING COMPONENTS

6.1 SERIES COMBINATION

Since fan-out systems are being considered, the most common combination of components will be the series combination (Figure 5-2).



Figure 5-2. Series Combination of Components

Derived next are the state probabilities, as well as the failure and repair rates for this combination. $P_i(j)$ is used to indicate the $i^{\underline{th}}$ state of the $j^{\underline{th}}$ component; a_j, etc., to indicate the appropriate failure or repair rate for the $j^{\underline{th}}$ component; and a superscripted parenthetical numeral to indicate the probability or rate for the combination of components (a superscripted (2), for example, indicating a series of two components).

First, it is obvious that for the correct operation of the series combination, both components must be operating; thus

$$P_0^{(2)} = P_0(1)\ P_0(2)$$

Next, for the combination to produce a false alarm, there are two combinations of events possible: component 2 fails in an on condition regardless of the state of component 1; or, component 1 fails in an on condition and component 2 is operating normally. Thus:

$$P_1^{(2)} = P_1(2) + P_1(1)\ P_0(2)$$

Finally, the combination can fail in an off condition in two ways: component 2 can fail in an off condition no matter what the state of component 1; or, component 1 can fail in an off condition while 2 is operable. Thus

$$P_2^{(2)} = P_2(2) + P_2(1)P_0(2)$$

It can be readily verified that

$$\Sigma P_i^{(2)} = 1$$

as required by probability theory.

To determine the failure and repair rates of the series combination, it is necessary to first determine the combined failure rates, i.e., $[a^{(2)} + b^{(2)}]$. This is known[1] to be

$$[a^{(2)} + b^{(2)}] = \sum_i (a_i + b_i)$$

Then, since

$$P_0^{(2)} = \frac{m^{(2)}}{a^{(2)} + b^{(2)} + m^{(2)}}$$

$$m^{(2)} = \frac{P_0^{(2)} \Sigma (a_i + b_i)}{1 - P_0^{(2)}}$$

it follows immediately that

$$a^{(2)} = P_1^{(2)} [a^{(2)} + b^{(2)} + m^{(2)}]$$

and

$$b^{(2)} = P_2^{(2)} [a^{(2)} + b^{(2)} + m^{(2)}]$$

The extension to n components follows by iteration.

---

1. Ibid., p. 77.

6.2 PARALLEL REDUNDANT COMPONENTS

Considered next are the parallel redundant combination of two components as in Figure 5-3. For simplicity of presentation, both components are considered identical, but the extension to different components is trivial.

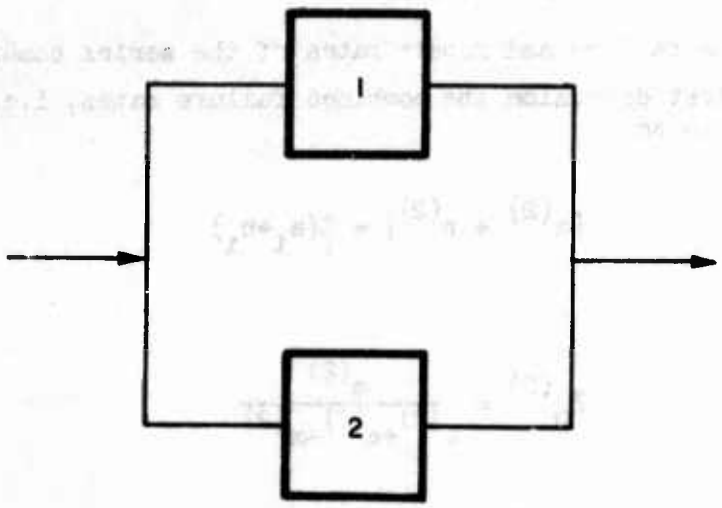


Figure 5-3. Parallel Redundant Combination of Components

Proceeding as in Section 6.1, $P_0^{(2)}$ is possible only if both components are operable, or either component is operable and the other has failed in an off condition, thus

$$P_0^{(2)} = P_0^2 + 2P_0P_2$$

$P_1^{(2)}$ is given by the probability of either component failing in an on condition regardless of the state of the other less the probability of both failing in an on condition at the same time, thus

$$P_1^{(2)} = 2P_1 - P_1^2$$

$P_2^{(2)}$ is given by the fact that both components must be in the no alarm state thus

$$P_2^{(2)} = P_2^2$$

To determine the rates for this configuration, it has been shown (for identical components) that[1]

$$[a^{(2)}+b^{(2)}] = \frac{2(a+b)}{3(a+b)+m}$$

Thus:

$$m^{(2)} = \frac{P_0^{(2)}[a^{(2)}+b^{(2)}]}{1-P_0^{(2)}}$$

and $a^{(2)}$ and $b^{(2)}$ are found as in the series configuration.

7.0 MODEL SYNTHESIS

7.1 FUNDAMENTAL CONSIDERATIONS

In developing the methodology for model synthesis, it must be assumed that the basic system configuration has already been determined. In other words, the development of a reliability model presupposes the existence of a system model. This system model then becomes the framework upon which the reliability characteristics of the components are superimposed to determine the ability of the configuration to meet system reliability requirements, or perhaps even to determine the reliability requirements of the components from overall system reliability requirements.

7.2 NOTATION

7.2.1 System Block Diagram

A block diagram of a system is merely a diagram of the components of the system and their interconnecting links.[2] The symbol for a component will simply be a block with the name of the component and an identifying number. One convention

---

1. Ibid., p. 139.

2. See Section 3.1 for the definition of "component" upon which this section is based.

must be observed: identical components must have the same identifying number, and are numbered serially from the originator to the ultimate receiver. This allows for a simplification later in the transition to reliability models.

Figure 5-1 shows a three-level fan-out network consisting of a Central Warning Point or CWP, Repeater Warning Points or RWP, and Terminal Warning Points or TWP. According to the above convention, the TWP connected directly to the CWP is numbered 3 rather than 2 because it is not a RWP, but a TWP, and, thus, is identical with all other TWPs. The diagram in Figure 5-1 can be further simplified by condensation across similar functional levels; this type of simplification is shown in Figure 5-4. Note that the replications of each component in a given level is indicated in parentheses after the identity number;

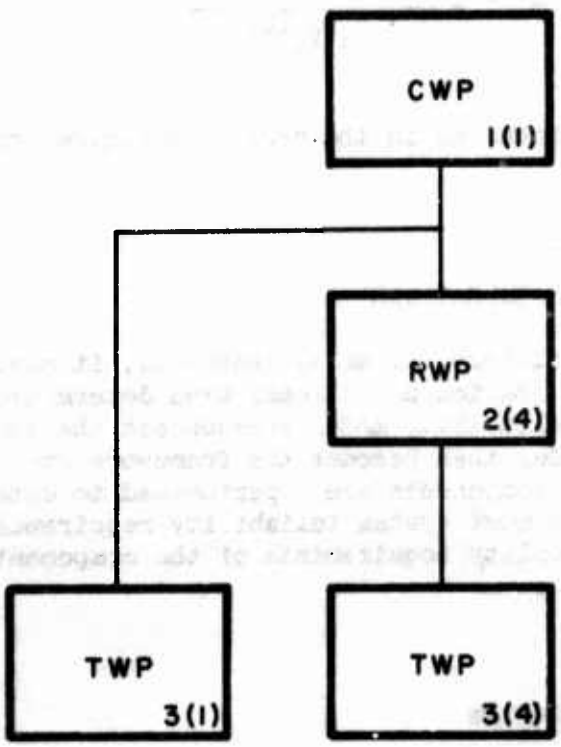


Figure 5-4. Condensation of Network Shown in Figure 5-1.

also, that components that are not in the same series, even though they are in the same level, are shown separately. Thus the right hand TWPs in Figure 5-4 are all identical and follow the same pattern in that four are attached to each

RWP, which is in turn attached to the CWP. The left hand TWP is separated from the others because it is attached directly to the CWP, and not to an RWP. Note also that the parenthetical number refers to the number attached to a given component in the level above it, not the aggregate attached to all the components in the level above. If a different number of TWPs were attached to the RWPs, then a separate block would have to be drawn for each different combination. If, however, the number of TWPs connected to the RWPs is sufficiently large and does not vary too much (in the statistical sense), then one representation of the TWP would be sufficient with the number of replications being the average for all the RWPs.

One further note on redundancy: if, at any level, the replications in a box indicate redundancy, this is designated in the lower right hand corner by an R.

7.2.2 Reliability Model Synthesis

From the condensed system block diagram, it is an easy step to the reliability model. One merely inserts, in the condensed system block diagram, blocks for the communications channels indicating which blocks it connects and its degree of replication. Thus, if a channel connects, say, block 2 with block 3, and if there are four blocks 3, the block representing the connecting channel would bear the identification (2, 3)(4). The reliability model for the warning system in Figures 5-1 and 5-4 is given in Figure 5-5. (The cautionary note and notational conventions for redundancy given in Section 7.2.1, above, must also be observed for communication blocks.) Note that from this point on, no distinction is made between communication links and components since both types are now described in exactly the same manner, i.e., in terms of their failure and repair rates.

The reliability model shows all the unique chains in the warning network. Working with these chains then allows the utilization of theorem in probability theory stating that the probability of the simultaneous occurrence of independent events is equal to the product of the probabilities of the individual occurrence of each. Thus, the probability of successful operation of a chain is the product of the probabilities of successful operation of each component.

8.0 AN EXAMPLE

8.1 THE MODEL

Next the developed methodology is applied to a hypothetical National Warning Dissemination System (NWDS). The application of the reliability model to a hypothetical system is necessary because of the paucity of data concerning the reliability of present warning systems. The system consists of the following components:

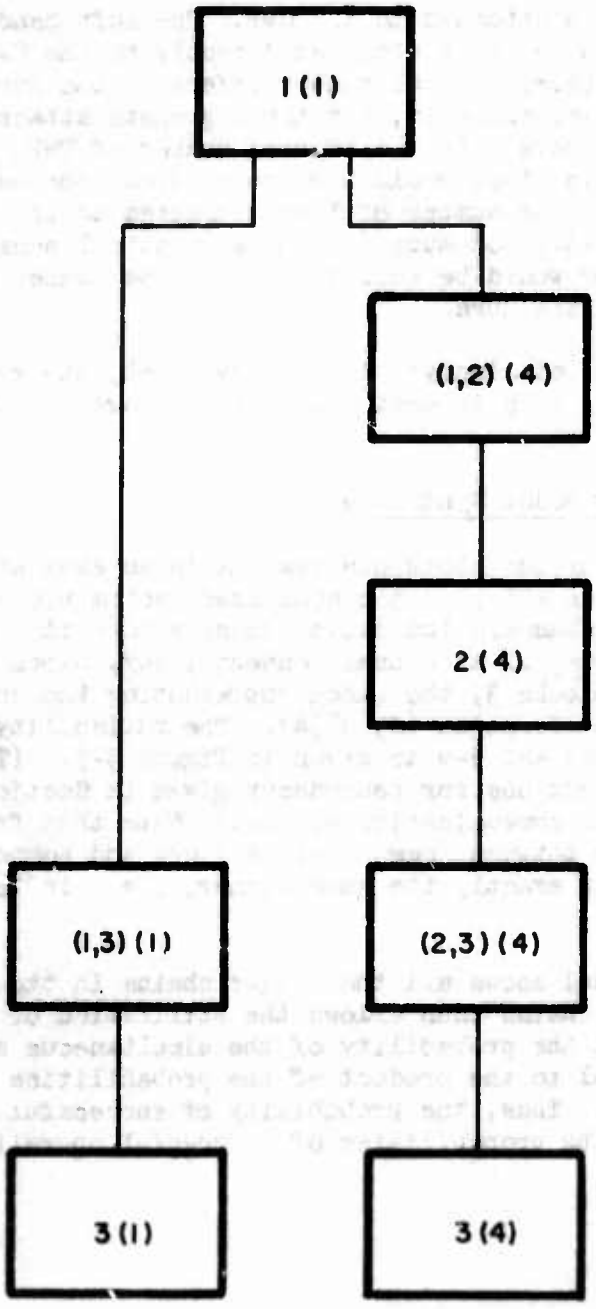


Figure 5-5. Reliability Model for Warning System in Figures 5-4 and 5-5

1. National Warning Points (NWP). There are two NWPs operating in a standby redundant configuration. They are identical and have the following failure characteristics:

a. MTTF(1) = 40 years
b. MTTF(2) = 20 years
c. MTTR = 1 hour

They are individually connected to a National Warning Center by communication channels with the following characteristics:

a. MTTF(1) = 275 years
b. MTTF(2) = 2.75 years
c. MTTR = 1 hour

2. National Warning Center (NWC). The NWC receives the warning information from the NWPs and disseminates it to the Sectional Warning Centers. The characteristics of the NWC are as follows:

a. MTTF(1) = 20 years
b. MTTF(2) = 20 years
c. MTTR = 6 hours

The characteristics of the communication channels to the Sectional Warning Centers are:

a. MTTF(1) = 275 years
b. MTTF(2) = 2.75 years
c. MTTR = 2 hours

3. Sectional Warning Centers (SWC). There are eight SWCs. Each supplies information to 6,250,000 Terminal Warning Points and eight Local Warning Centers. The characteristics of the SWCs are as follows:

a. MTTF(1) = 20 years
b. MTTF(2) = 10 years
c. MTTR = 6 hours

The communication channels to the Local Warning Centers and the Terminal Warning Points are identical and have the following characteristics:

a. MTTF(1) = 275 years
b. MTTF(2) = 2.75 years
c. MTTR = 3 hours

4. Local Warning Centers (LWC). The LWCs are each connected to 312,500 Terminal Warning Points. They have the following characteristics:

a. MTTF(1) = 10 years
b. MTTF(2) = 10 years
c. MTTR = 8 hours

Its communication channels with the Terminal Warning Points have the same characteristics as the SWC-to-LWC channel.

5. Terminal Warning Points (TWP). The TWP are inexpensive home warning devices, and are, therefore, less reliable devices than those used in the rest of the system. There are a total of 70 million in the system. They have the following characteristics:

a. MTTF(1) = 5 years
b. MTTF(2) = 5 years
c. MTTR = 7 days

The condensed system diagram is presented in Figure 5-6 and the failure and repair characteristics are converted to rates and presented in Table 5-2. The reliability model is presented in Figure 5-7. (The double box at the top of the diagram indicates that 1 and (1, 2) are serially connected and the configuration 1(1, 2)(2) is redundant.)

One further note on testing: all components except the LWCs and the TWPs are assumed to be continually monitored. The LWCs are tested every ten days with no downtime for the test. The TWPs are tested in a manner which requires downtime of five minutes for the test.

8.2 THE WORKSHEET

The layout of the worksheet to be employed in the analysis is shown in Figure 5-8 (the known parameters from the preceding section have been inserted). The computational methods employed (keyed to the column number) are as follows:

Column 1 - Given.
Column 2 - Given.
Column 3 - Given.
Column 4 - Absolute probability of false alarm failure (Section 5.1, eq. 8).

$$P_{\perp} = \frac{a}{a+b+m}$$

Table 5-2. Failure and Repair Rates per Day for NWDS Components and Links

Component or link	a	b	m
1	0.00007	0.00014	24.0
1.2	10^{-5}	0.001	24.0
2	0.00014	0.00014	4.0
2.3	10^{-5}	0.001	12.0
3	0.00014	0.00027	4.0
3.4	10^{-5}	0.001	8.0
4	0.00027	0.00027	3.0
4.5	10^{-5}	0.001	8.0
3.5	10^{-5}	0.001	8.0
5	0.00055	0.00055	0.14286

Note: $a = \frac{1}{MTTF(1)}$

$b = \frac{1}{MTTF(2)}$

$m = \frac{1}{MTTR}$

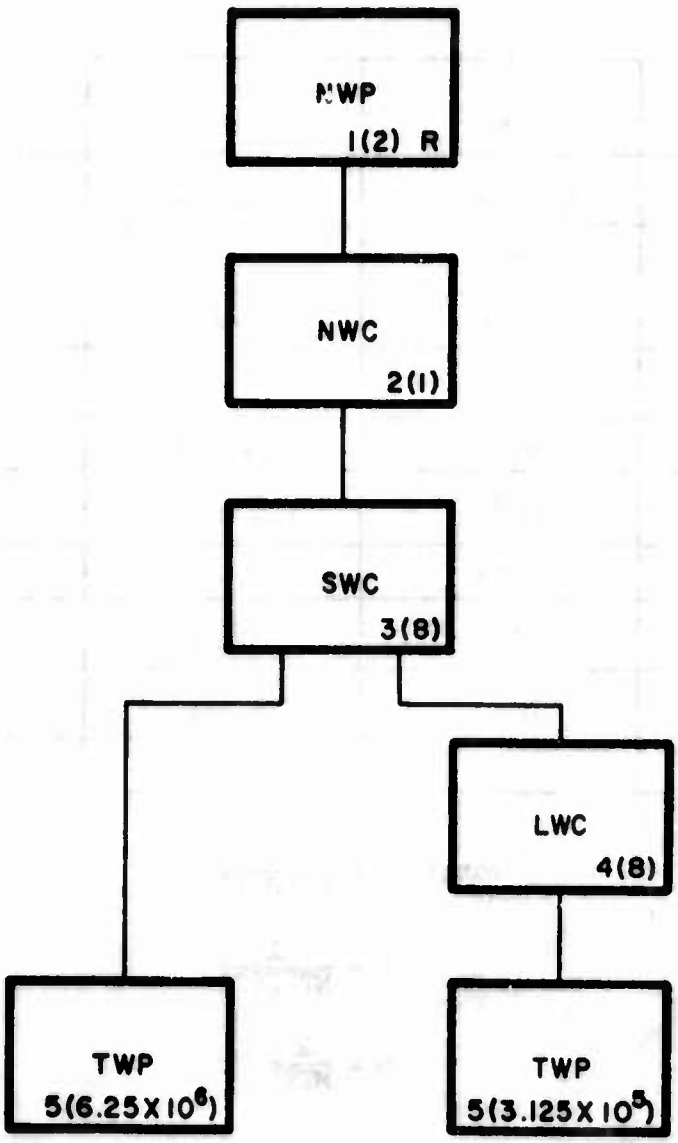


Figure 5-6. Condensed Network of the Hypothetical National Warning Dissemination System (NWDS)

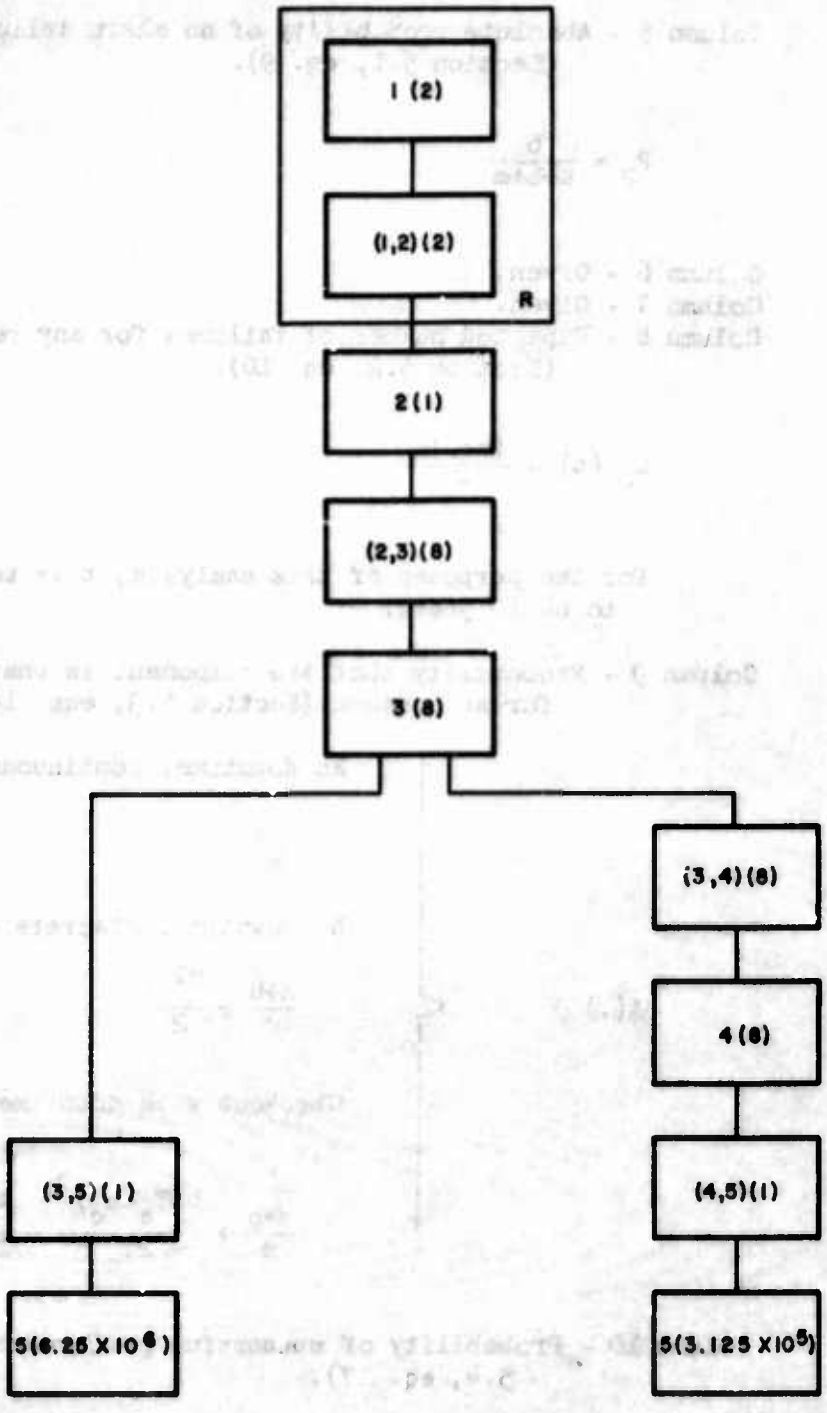


Figure 5-7. Reliability Model for NWDS

Column 5 - Absolute probability of no alarm failure (Section 5.1, eq. 9).

$$P_2 = \frac{b}{a+b+m}$$

Column 6 - Given.
Column 7 - Given.
Column 8 - Expected number of failures for any reason (Section 5.2, eq. 10).

$$u_{00}(t) = \frac{(a+b)mt}{a+b+m}$$

For the purposes of this analysis, t is taken to be 10 years.

Column 9 - Probability that the component is unavailable for any reason (Section 5.3, eqs. 14-16).

$$A(.) \approx \begin{cases} \text{No downtime, continuous checkout:} \\ \quad \frac{a+b}{m} \\ \text{No downtime, discrete checkout:} \\ \quad \frac{a+b}{m} + \frac{bT_c}{2} \\ \text{Checkout with downtime} \\ \quad \frac{a+b}{m} + \frac{b(T_c-t_c)^2}{2T_c} + \frac{t_c}{T_c}\left(1-\frac{a}{m}\right) \end{cases}$$

Column 10 - Probability of successful performance (Section 5.4, eq. 17).

$$S = [1-A(.)](1-P_2)$$

WARNING SYSTEM RELIABILITY EVALUTION

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
COMPONENT	a	b	m	P_1	P_2	t_c	T_c	Voo(t)	A(.)	S	Down	E(1)	E(2)	Affected
1(1)	.0007	.00014	24.0			0	0							70×10^6
(1,2)(1)	10^{-5}	10^{-3}	24.0			0	0							70×10^6
1(1,2)(2)						0	0							70×10^6
2	.00014	.00014	4.0			0	0							70×10^6
(2,3)	10^{-5}	10^{-3}	12.0			0	0							8.75×10^6
3	.00014	.00027	4.0			0	0							8.75×10^6
(3,4)	10^{-5}	10^{-3}	8.0			0	0							3.125×10^6
(3,5)	10^{-5}	10^{-3}	8.0			0	0							6.25×10^6
4	.00027	.00027	3.0			0	0							3.125×10^6
(4,5)	10^{-5}	10^{-3}	8.0			0	0							3.125×10^6
5	.00055	.00055	.14286			.00347	3.552							

Figure 5-8 Reliability Worksheet

(Page 5-36 blank)

Column 11 - Downtime in days per 10 years.

(Down) = 3650A(.)

Column 12 - Expected number of false alarm failures (Section 5.2, eq. 11).

$$E(1) = \frac{a}{a+b} \cdot u_{00}(t)$$

Column 13 - Expected number of no alarm failures (Section 5.2, eq. 12).

$$E(2) = \frac{b}{a+b} \cdot u_{00}(t)$$

Column 14 = Terminals affected by an individual component at each level. (from Figure 5-7). The figure represents the number of TWPs that are directly controlled by the given level.

The results of the computations are shown in Figure 5-9. The figures on line three were derived by first computing the state probabilities and failure and repair rates for a series configuration as described in Section 5.1 for the configuration 1(1, 2)(1), and then again for the switched redundant configuration as in Section 6.3 for the configuration 1(1, 2)(2).

It is interesting to note the figure at the botton of column 10. This figure 0.98536, is the probability that an individual TWP is properly activated and operates if an actual warning is issued by the NWC. This is computed by taking the weighted product of the values of S in the two branches of the hypothetical system. This essentially says that about 1.5 percent of the population is continually at risk because of improper system functioning.

8.3 ANALYSIS AND INTERPRETATION OF RESULTS

With the figures developed in Section 8.2, it is now possible to determine the total number of false alarm and no alarm failures that can be expected to occur over a given period of time (ten years for the example) for all components: the average number of terminals affected by each such failure: and the average duration of each such failure. It is assumed that when a component fails, the portion of the system below that component operates in a normal manner, i.e., if a false alarm is generated in a SWC, the LWCs and TWPs attached to it disseminates the alarm as if it were a valid alarm. It is also assumed that the probability of the simultaneous failure of more than one component at any level (except the TWPs) is so small as to be negligable.

As noted in Section 5.5, the probability, S, that the system will properly disseminate a legitimate warning is given by the product of the values of S; for each level, or

$$S = \prod_i S_i \qquad (21)$$

(In the example, S = 0.98536.) This value, in reality, is the probability that any randomly selected TWP will receive and disseminate a legitimate warning. This is the first measure of system performance.

The next area investigated is false alarms. Investigated first is the number of terminals affected by the failing of the $i^{\underline{th}}$ component into an on condition; second, the total expected failures into an on condition of all like components over a given time period; and, last, the average duration of downtime for that component. The last figure does not give the duration of a false alarm, but, rather, gives a time during which a no alarm condition prevails, for a component that fails into an on condition precludes the use of components in the network below that component for warning and thus presents essentially a failed off condition for the duration of repairs to the component that failed into an on condition. The calculations for the TWPs are noted separately in the results because the effect of their multiplicity would tend to dilute the results of computations for the control network.

To determine the average number of terminals affected by false alarms at any level, the procedure is as follows. Consider Figure 5-7 of Section 8.1, above. The components of the model are numbered such that the numbers follow the flow of information from the source to the ultimate destination. Following the failure of component 2 into an on condition, for instance, all of the terminals in the system would receive a false alarm if all the components whose number is greater than 2 perform properly. Following the failure into an on condition of one of the components labeled 4, only 0.446 percent of the terminals would receive the false alarm if all the TWPs performed properly. The point being that a false alarm is transmitted to the terminals of the system only if those components in the chain below the failing component operate as designed.

Let p_i be the terminals under the $i^{\underline{th}}$ component; N_i, the number of $i^{\underline{th}}$ components in the system; $E(1)_i$, the expected number of false alarms; and S_j, the ultimate reliability of the $j^{\underline{th}}$ component. Then the terminals (M_i) affected by a false alarm of the $i^{\underline{th}}$ component is

$$M_i(1) = p_i \prod_{j>1} S_j \qquad (22)$$

WARNING SYSTEM RELIABILITY EVALUTION

	1	2	3	4	5	6	7	8	9	10	11	12	13	14
COMPONENT	a	[illegible]	m	P_1	P_2	t_c	T_c	Voo(t)	A(.)	S	Down	E(1)	E(2)	Affected
1(1)	.0007	.00014	24.0	2.9×10^{-6}	5.8×10^{-6}	0	0	.76649	8.75×10^{-5}	0.99991	.32	.26	.51	70×10^{6}
(1,2)(1)	10^{-5}	10^{-3}	24.0	0.4×10^{-6}	4.2×10^{-5}	0	0	3.68634	4.21×10^{-6}	0.99992	.15	.04	3.65	70×10^{6}
1(1,2)(2)	72×10^{-10}	548×10^{-8}	23.846	3×10^{-10}	23×10^{-10}	0	0	.00023	~0	~1.0	~0	.00003	.00020	70×10^{6}
2	.00014	.00014	4.0	3.5×10^{-5}	3.5×10^{-5}	0	0	1.02192	7.0×10^{-5}	0.99989	.26	.51	.51	70×10^{6}
(2,3)	10^{-5}	10^{-3}	12.0	0.8×10^{-6}	8.3×10^{-5}	0	0	3.68618	8.42×10^{-5}	0.99984	.31	.04	3.65	8.75×10^{6}
3	.00014	.00027	2.0	3.5×10^{-5}	6.7×10^{-5}	0	0	1.49634	10.25×10^{-5}	0.99983	.37	.51	.99	8.75×10^{6}
(3,4)	10^{-5}	10^{-3}	8.0	1.2×10^{-6}	12.50×10^{-5}	0	0	3.68603	12.63×10^{-5}	0.99975	.46	.04	3.65	3.125×10^{5}
(3,5)	10^{-5}	$.10^{-3}$	8.0	1.2×10^{-6}	12.50×10^{-5}	0	0	3.68603	12.63×10^{-5}	0.99975	.46	.04	3.65	6.25×10^{6}
4	.00027	.00027	3.0	.00009	.00009	0	0	1.97064	.00153	0.99838	5.58	.99	.99	3.125×10^{5}
(4,5)	10^{-5}	10^{-3}	8.0	1.2×10^{-6}	12.50×10^{-5}	0	0	3.68603	12.63×10^{-5}	0.99975	.46	.04	3.65	3.125×10^{5}
5	.00055	.00055	.14286	0.00770	0.00770	.00347	3.552	3.98342	.00964	0.98657	35.19	1.99	1.99	
										0.98536				

Figure 5-9. Completed Reliability Worksheet

and the average number of terminals (M(1)) affected by a false alarm at any level by any component at that level is

$$(23) \qquad M(1) = \frac{\sum_i M_i(1) N_i E(1)_i}{\sum_i N_i E(1)_i}$$

The total number of such occurrences, $\overline{E(1)}$,

$$(24) \qquad \overline{E(1)} = \sum_i N_i E(1)_i$$

and the average downtime, $t_d(1)$, is

$$(25) \qquad t_d(1) = \frac{\sum_i N_i E(1)_i \frac{1}{m_i}}{\overline{E(1)}}$$

N_i and p_i are taken from the reliability model (Figure 5-7).

Finally, for the no alarm situations, the procedure is as above except that system performance below the failed component need not be taken into consideration because the terminals are affected regardless of whether the subordinate system functions properly. Thus

$$(26) \qquad M_i(2) = p_i$$

$$(27) \qquad M(2) = \frac{\sum_i M_i(2) N_i E(2)_i}{\sum_i N_i E(2)_i}$$

$$(28) \qquad \overline{E(2)} = \sum N_i E(2)_i$$

and

$$(29) \qquad t_d(2) = \frac{\sum_i N_i E(2)_i \frac{1}{m_i}}{\overline{E(2)}}$$

The average downtime, t_d, for any type failure is then given by

$$(30) \qquad t_d = \frac{t_d(1)\overline{E(1)} + t_d(2)\overline{E(2)}}{\overline{E(1)} + \overline{E(2)}}$$

and, of course, the total expected number of failures, $\overline{E}$, is

$$(31) \qquad \overline{E} = \overline{E(1)} + \overline{E(2)}$$

and the average affected population, M, is

$$(32) \qquad M = \frac{M(1)\overline{E(1)} + M(2)\overline{E(2)}}{\overline{E(1)} + \overline{E(2)}}$$

The computational form is given in Figure 5-10, and the results for the example are contained in Figure 5-11. The computational methods employed (keyed to column number) are as follows:

Column 1 - Terminals affected (Column 14, Figure 5-9).

Column 2 - The probability of successful propagation of a warning, given by

$$S_i = \prod_{j>i} S_j$$

where i is the $i^{\underline{th}}$ level and j is the index of the levels below i.

Column 3 - $M_i(1)$ represents the average number of terminals affected by a false alarm generated at the $i^{\underline{th}}$ level (given by equation 22), the product of columns 1 and 2.

Column 4 - The expected number of false alarms generated by this level, given by column 12, Figure 5-9.

Column 5 - The expected number of no alarm situations originating at this level, given by column 13, Figure 5-9.

Column 6 - The total number of components at this level from Figure 5-6.

Column 7 - The reciprocal of the MTTR for the i^{th} component from Table 5-2.

Column 8 - The expected number of false alarms for the i^{th} component. The sum of this column gives E(1), given by equation 28.

Column 9 - The terminals affected by a false alarm at the i^{th} level. The sum of this column divided by the sum of column 8 given the average number of terminals, M(1), affected by a false alarm at any level (equation 23).

Column 10 - Total downtime caused by false alarms at the i^{th} level. The sum of this column divided by the sum of column 8 gives the average downtime, $t_d(1)$, for each false alarm (equation 25).

Column 11 - The expected number of no alarm situations for the i^{th} component. The sum of this column gives E(2), given by equation 28.

Column 12 - The terminals affected by a no alarm situation caused by i^{th} component. The sum of this column divided by column 11 gives the average number of terminals, M(2), affected by a no alarm situation at any level (equation 27).

Column 13 - Total downtime caused by a no alarm situation at the i^{th} level. The sum of this column divided by column 11 gives the average downtime, $t_d(2)$, for each no alarm situation (equation 29).

Column 14 - The total expected number of failures, either false alarms or no alarm situations. This is given by equation 31.

Column 15 - The average number of terminals affected for each failure, given by equation 32.

Column 16 - The average downtime for either type of failure, given by equation 30.

Note that the control network computations are separate from the TWP computations because a failure in the control net affects a block of contiguous TWPs, while the TWP failures are at random and generally are not concentrated in any one area.

The summary failure data for the control net is then

$$E = 671.10$$

$$M = 1.20 \times 10^6$$

$$t_d = 0.165 \text{ days}$$

$$\approx 4 \text{ hours}$$

where

$\bar{E}$ = the total failures of either kind for a 10 year period (equation 31)

M = the average number of terminals affected by for any type of failure, and

For the TWPs, the summary data is

$$\bar{E} = 278.6 \times 10^6$$

$$M = 1$$

$$t_d = 7 \text{ days}$$

From the summary data, several rather startling inferences can be drawn about the hypothetical system under evaluation. It can be expected that each TWP must be repaired (or replaced) about three times during a ten-year period. There will be about 76,320 TWPs failing each day, half giving false alarms in the process. An average of 1.19 million TWPs will be unable to disseminate warning because of control system failures about every six days. False alarms will be disseminated to an average of 1.31 million TWPs about every fifty days. It is obvious that any warning system developed must be much more reliable than the hypothetical NWDS.

8.4 ALLOCATION OF RELIABILITY TO THE NWDS

If instead of the given parameters, the only required number was a system S of 0.999, the system designer is faced with the allocation problem discussed in Section 5.5, above. Considering the longest chain in the network, e.g.,

WARNING SYSTEM JEOPARDY ANALYSIS

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
COMPONENT	p_i	πS_i	$M_i(1)$	$E_i(1)$	$E_i(2)$	N_i	m_i	4 X 6	3 X 8	8/7	5 X 6	1 X 11	11/7			
(1(1,2)2)	70×10^6	.98560	68.99×10^6	.00003	.00020	1	23.946									
2	70×10^6	.9857[illegible]	69.00×10^6	.51	.51	1	4.0									
(2,3)	8.75×10^6	.98587	8.63×10^6	.04	3.65	8	12.0									
3	8.75×10^6	.98604	8.63×10^6	.51	.99	8	4.0									
(3,4)	3.125×10^5	.98472	3.08×10^5	.04	3.65	64	8.0									
4	3.125×10^5	.98632	3.08×10^5	.99	.99	64	3.0									
(4,5)	3.125×10^5	.98657	3.08×10^6	.04	3.65	64	8.0									
(3,5)	6.25×10^6	.98657	6.17×10^6	.04	3.65	8	8.0									
CONTROL NET SUMMARY								$\overline{E}(1)$	M(1)	$t_d(1)$	$\overline{E}(2)$	M(2)	$t_d(2)$	$\overline{E}$	M	t_d
TERMINAL SUMMARY								$\overline{E}(1)$	M(1)	$t_d(1)$	$\overline{E}(2)$	M(2)	$t_d(2)$	$\overline{E}$	M	t_d
5	1	1	1	1.99	1.99	70×10^6	.14286									

Figure 5-10

WARNING SYSTEM JEOPARDY ANALYSIS

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
COMPONENT	pi	$\sum S_i$	M_i (1)	E_i(1)	E_i(2)	N_i	m_i	4 X 6	3 X 8	8/7	5 X 6	1 X 11	11/7			
(1(1,2)2)	70×10^{6}	.98560	68.99×10^{6}	.00003	.00020	1	23.846	.00003	.00207	~0	.00020	1.40×10^{4}	~0			
2	70×10^{6}	.98571	69.00×10^{6}	.51	.51	1	4.0	.51	35.19×10^{6}	.12750	.51	35.70×10^{6}	.12750			
(2,3)	8.75×10^{6}	.99587	8.68×10^{6}	.04	3.65	8	12.0	.32	2.76×10^{6}	.04000	29.20	2.56×10^{7}	2.43333			
3	8.75×10^{6}	.98604	8.68×10^{6}	.51	.99	8	4.0	4.08	35.21×10^{6}	1.02000	7.92	6.93×10^{7}	1.98000			
(3,4)	3.125×10^{5}	.98472	3.08×10^{5}	.04	3.65	64	8.0	2.56	7.88×10^{5}	.32000	233.60	73.0×10^{6}	29.20000			
4	3.125×10^{5}	.98632	3.09×10^{5}	.99	.99	64	3.0	63.36	19.51×10^{6}	21.12000	63.36	19.8×10^{6}	21.12000			
(4,5)	3.125×10^{5}	.98657	3.08×10^{5}	.04	3.65	64	8.0	2.56	7.89×10^{5}	.32000	233.60	73.0×10^{6}	29.20000			
(3,5)	6.25×10^{6}	.98657	6.17×10^{6}	.04	3.65	8	8.0	0.32	1.97×10^{6}	.04000	29.20	1.83×10^{8}	3.65000			
									96.22×10^{6}	22.9875		7.088×10^{9}	8771083			
CONTROL NET SUMMARY								$\bar{E}$ (1)	M (1)	t_d (1)	$\bar{E}$ (2)	M (2)	t_d(2)	$\bar{E}$	M	t_d
								73.71	1.31×10^{6}	0.31186	597.39	1.19×10^{6}	.14682	671.10	1.20×10^{6}	0.16494
										$\approx 7\frac{1}{2}$ hrs			$\approx 3\frac{1}{2}$ hrs			≈ 4 hrs
TERMINAL SUMMARY								$\bar{E}$ (1)	M (1)	t_d (1)	$\bar{E}$ (2)	M (2)	t_d(2)	$\bar{E}$	M	t_d
5	1	1	1	1.99	1.99	70×10^{6}	.14286	139.3	1	7	139.3	1	7	278.6	1	7
								$\times10^{6}$			$\times10^{6}$			$\times10^{6}$		

Figure 5-11

the one containing the LWCs, there are eight components in the series. If there are no relative importances established, then the required performance, S_i, of each component would be (Section 5.5, eq. 12)

$$S_i = S^{\frac{1}{8}} = (0.999)^{\frac{1}{8}} = 0.999875$$

If, on the other hand, relative importances are established, the procedure is as follows. Suppose the components were assigned importances as in table 5-3.

Table 5-3. Relative Importance of Components

Component	Importance (E_i)
1(1,2)(2)	100
2	100
(2,3)	100
3	75
(3,4)	75
4	50
(4,5)	50
5	40

The normalizing constant m is first computed (Section 5.5, eq. 21)

$$m = \frac{1}{n} \sum \frac{1}{E_i}$$

$$= \frac{1}{8}\left(\frac{3}{100} + \frac{2}{75} + \frac{2}{50} + \frac{1}{40}\right)$$

$$= 0.01521$$

Since (Section 5.5, eq. 20)

$$k_i = \frac{1}{mn\ E_i}$$

then

$$k_i = \frac{1}{0.12168E_i}$$

Table 5-4 gives the k_i and the suitable S_i for each given importance level (Section 5.5, eqs. 19, 20).

Table 5-4. Required Reliabilities with Importance

Importance (E_i)	k_i	S_i
100	0.08219	0.999918
75	0.10959	0.999890
50	0.16439	0.999833
40	0.20547	0.999794

Note that for the most important component, the unreliability (the complement of the reliability) must be decreased ten percent over the case where importance figures were not assigned; while, for the least important item, an increase in unreliability of ten percent is allowed. In terms of component design, these factors could be critical.

CHAPTER SIX

FEASIBILITY OF USING COMMUNICATIONS SATELLITES FOR PUBLIC ALERTING AND WARNING

1.0 INTRODUCTION

This chapter reports the findings of a brief review of the feasibility of using satallites for public alerting and warning.[1] Two separate, but related, approaches have been made to the problem:

1. Determining the capabilities of communications satellites currently operational or planned for service in the next several years.

2. Evaluating any types of service related to public alerting and warning that may have been planned or proposed.

The review included a scrutiny of published policy statements of the organizations concerned with satellite communications--principally the Defense Communications Agency (DCA), the National Aeronautics and Space Agency (NASA), and the Communications Satellite Corporation.[2]

2.0 CONCLUSIONS AND RECOMMENDATIONS

As a result of the review, it has been concluded that:

1. Technical Feasibility of Direct Source Alerting and Warning.

It appears that using satellites for direct public alerting and warning is technically promising. Currently operational synchronous satellites (especially Syncom 3) may be modifiable to provide public alerting and warning; if such modification is not possible, then special-purpose alerting and warning satellites appear to be within current technology.

---

1. This chapter replaces Feasibility of Using Communications Satellites for Public Alerting and Warning, which was originally published as TM-L-1960/081/00, dated 15 December 1964.

2. Since the original publication of the findings reported in this chapter, several agencies have manifested interest in direct broadcasting from a satellite to entertainment-type receivers. This chapter is republished, nevertheless, because it is felt that the conclusions reached are still valid. Several footnotes have been added to indicate changes that have occurred since the original publication of the report.

2. Technical Feasibility of Satellites as Warning Relay Stations.

The possible use of special satellites to relay alert signals and warning information between national control points and regional or local public alerting and warning transmitters is technically simpler than that of direct alerting and warning. This conclusion is valid if only because of the resulting reduction in the number of receivers and thus the greater allowable expense for each receiver and antenna at a relaying station.

3. Operational Undesirability of Satellites for Alerting and Warning.

Despite the technical feasibility of direct home alerting and warning and of indirect relay service, it must be concluded that using satellites for either type of service is operationally undesirable. This conclusion is based upon the vulnerability of suitable synchronous satellite systems to direct destruction and, perhaps more important, to easy spoofing and jamming, either for harassment or as an adjunct to an attack.

It is recommended, therefore, that no further effort be applied to satellites for either direct public alerting and warning or for point-to-point alert and warning relaying from the national level to regional and/or local levels. This conclusion should not preclude further research on the potential of satellites to provide OCD communications, especially in conjunction with the forthcoming DOD military communications satellite system.

3.0 REVIEW OF SATELLITE COMMUNICATIONS SERVICES

As of the date of the original publication of the information in this chapter, there was no indication that organizations such as DCA, NASA, and Communications Satellite Corporation had formulated plans for developing satellite systems capable of transmitting directly to home-type receivers. The review on which this chapter is based indicated that the plans of these organizations called for providing point-to-point service between special-purpose ground stations; this service serves primarily as an adjunct to conventional landline and radio communications.[1] Such service would be derived from medium-altitude, random-orbit satellites; high-altitude, synchronous-orbit satellites; or a mix of both. In fact, even a superficial review of the characteristics of random-orbit and synchronous-orbit satellites indicates that these vehicles, as currently employed, cannot be used for home alerting and warning. Random-orbit satellites have the following limitations:

1. Since that time there have been several expressions of interest in direct broadcasting to home-type receivers. cf., "Direct Broadcast Satellite for Home Reception," Electronics World, (75) 2 February 1966, p. 69; "Putting Space to Work to Educate the World," Business Week, 25 December 1965, p. 17.

1. They are subject to outages resulting from limited coverage.

2. They require many satellites to approach full coverage.

3. They employ expensive, complex tracking antennas and sensitive, high-gain receivers.

These characteristics, especially the latter, appear to remove random-orbit satellites from consideration as part of alerting and warning systems.

Synchronous-orbit satellites, as currently employed, provide extensive predictable coverage. Nearly world-wide service is feasible from three satellites. Systems using this type of satellite are, however, subject to complete failure unless standby satellites are in orbit. The need for tracking is obviated, but receivers and antennas for current synchronous-orbit satellites are, nevertheless, expensive, complex high-gain devices. As currently employed, this type of satellite is also unsuitable for public alerting and warning.

4.0 TELEVISION BROADCASTING FROM SATELLITES

At the time of the original report, despite considerable popular speculations on the subject, only one significant proposal was found that related to alerting and warning--broadcasting television from a satellite directly into the house. This proposal was prepared by Radio Corporation of America, David Sarnoff Research Center, Princeton, N. J. The proposed system was outlined in five papers presented before the American Rocket Society in November 1962.[1]

The proposed RCA system is based upon synchronous-orbit satellites. The RCA system, however, uses state-of-the-art nuclear-reactor power supplies to increase transmitter power significantly. Its feasibility has been questioned for the 1970 time period. This system will, its proponents claim, transmit signals that can be received on home-type receivers using relatively inexpensive antenna systems.

1. Bond, Donald S., A System for Direct Television Broadcasting Using Earth Satellites, Radio Corporation of America, July 1962. Since the publication of the original report, several other proposals have also been developed for broadcasting television directly from satellites to house receivers. Cf., P. J. Klass, "RCA, GE Study TV Broadcast Satellites," Aviation Week and Space Technology (84) 2, 11 January 1966, pp. 115, 117, 119; Berry Miller, "Hughes Proposes TV Broadcast Satellite," Aviation Week and Space Technology, (82) 5-1 February 1965, pp. 75, 77. It must be pointed out that several of the proposed systems require more sophisticated receivers and/or antennas than are common for home receivers and would, more appropriately, qualify the proposed systems for community service or fringe-area service.

The RCA satellites would use transmitters with ratings to several kilowatts and with 3-mHz bandwidths. These transmitters would provide coverage of more than a million square miles. Such a satellite would weigh on the order of four tons. An atomic reactor (a SNAP-8 currently under development for the Atomic Energy Commission) would provide 60 kw of electrical power. The reactor would power the transmitters. It would also power ion-propulsion engines used to lift the satellite from a parking orbit of several hundred miles to synchronous altitude (22,300 miles). The parking orbit would be achieved using currently available Atlas or Titan boosters.

5.0 POSSIBLE APPLICATIONS TO ALERTING AND WARNING

The capability to transmit video is far in excess of the requirements that OCD has established for a radio-based alerting and warning system. National alerting and warning could be accomplished using a single voice channel. (Additional channels would probably be required to provide regional capabilities, since the requirement for selective responses to coded signals appears likely to increase receiver costs significantly.) Assuming that a minimal system could be built around a single 6-kHz voice channel, the bandwidth ratio of a 3mHz TV channel to a 6-kHz alerting and warning channel is 500 to 1. Decreasing bandwidth requirements for any communications system reduces transmitter power requirements. Transmitter power reduction decreases electrical power supply requirements. In a satellite system, these reductions in transmitter power and power supply capacity bring the capabilities within range of currently operational synchronous satellites.

Using the assumption that a 6-kHz voice channel provides adequate bandwidth for an alerting and warning system, data collected in the review of operational and planned satellites was analyzed. Only synchronous satellites were considered, since the problems of coverage and tracking inherent in random-orbit satellites are not eased by bandwidth reduction. Of the synchronous satellites operational or planned, Syncom 3 appears very promising. (It was placed in orbit in August 1964 and has been used to relay the 1964 Olympic Games to the United States.) Syncom 3 is currently equipped with four 4-watt transmitters. This satellite is currently operating a wide-band mode capable of transmitting video signals. It weighs less than 1,000 pounds and can be raised to synchronous-orbit using currently available boosters. It uses solar cells and batteries to provide electrical power. Chemical means will keep the satellite on station for approximately three years.

The four 4-watt transmitters can be regarded, for sake of analysis, as one 16-watt transmitter of comparable weight and power consumption. If a 500 to 1 reduction in bandwidth is traded for gain, it appears that Syncom 3 may be modifiable to provide national alerting and warning directly to the home via a simple UHF or VHF receiver and a home-type fixed antenna. If Syncom 3 modifications are not feasible, then direct home alerting does appear feasible with a specially designed satellite. It is impossible to determine at this time

whether the coverage attainable through a satellite similar to Syncom 3 would be marginal or whether it would be sufficiently in excess of capacity to allow for more than one 6-kHz channel. The only point that can be made is that an operational satellite does appear modifiable to provide the desired alerting and warning capability.

6.0 OPERATIONAL EVALUATION

Although direct alerting and warning via a satellite does appear technically feasible, it does not appear operationally desirable. A synchronous-orbit satellite must be used for home alerting to provide adequate coverage and to eliminate the need for tracking antennas. Such a system is clearly subject to potential destruction by an enemy. More significantly, it is subject to spoofing and jamming by an enemy. Use of crypto or pseudo-crypto equipment can protect against spoofing, but there is no protection against jamming. Any system that is subject to jamming provides an enemy with an invitation to exploit that weakness as either a harassing techinque or as an adjunct to an attack. The location in space allows nationwide jamming at a power level equal to that of our own signals. (Operational Russian boosters are capable of lifting payloads in excess of our boosters, so that interference might be at power levels in excess of our own signals.) Land-based alerting and warning systems do not provide an enemy with a location from which national jamming is feasible. Without sizeable expenditures of funds, a land-based system probably cannot be jammed from another land-based or shipboard installation, except on a local or regional basis. Any system with the obvious vulnerability of a satellite alerting and warning system is operationally undesirable.

The problem of disseminating signals from the federal level via satellite to regional transmitters (e.g., special low-frequency stations) or to local transmitters (e.g., broadcast stations) is technically simpler than the problem of direct home alerting. Such a system could provide a direct relay to a regional or local station. This type of service is also technically feasible.[1] It is

1. Since the original publication of the information in this study, several proposals have been formulated for satellite communications service related to the dissemination of warning from a federal location to regional and/or local warning points. Cf., "ABC Bids for Its Own Satellite," Broadcasting, 27 September 1965, pp. 56, 58; P. J. Klass, "Support Grows for Airline VHF "Comsat " Aviation Week and Space Technology, (83) 21, 22 November 1965, pp. 83-86; "Comsat Asks Industry to Submit Proposals for Multi-Purpose Satellite Able to Provide up to 6000 Two-Way Voice Circuits, or 10 TV Channels; Service Would Include TV Distribution, Air-Ground and Ship-Shore Links," Telecommunications Reports, (32) 4, 3 January 1966, pp. 1-2.

easier to achieve than a system that reaches the individual home because it deals with fewer receivers and allows a much larger expenditure or each receiver and antenna installation. This type of service, however, suffers from the same vulnerability to destruction, spoofing, and jamming that plagues a satellite home alerting and warning system.

APPENDIX A

BIBLIOGRAPHY

"ABC Bids for Its Own Satellite," Broadcasting, 27 September 1965, pp. 56, 58.

Barlow, Richard E. and Proschan, Frank, Mathematical Theory of Reliability, John Wiley and Sons, Inc., New York, New York, 1965.

Barrow, F. P., Report on Emergency Shutdown - Baton Rouge, Refinery, April 29, 1960.

Bellman, Richard, A Survey of the Mathematical Theory of Time-Lage, Retarded Control, and Hereditary Processes, The RAND Corp., R-256, 1 March 1954, Parzen, pp. 160 ff.

Bond, Donald S., Ed., A System for Direct Television Broadcasting Using Earth Satellites, Radio Corporation of America, 1 July 1962.

Brown, G. M., Space Radio Communication, Elsevier Publishing Company, Amsterdam, New York, and London, 1962.

Burke, Joseph R., "Passive Satellite Development and Technology," Astronautics and Aerospace Engineering, (1) 8, September 1963, 72-75.

Charyk, Joseph V., "Communications Satellite Corporation: Objectives and Problems," Astronautics and Aerospace Engineering, (1) 8, September 1963, 45-47.

Collins, J. Lawton, "Our Modern Military Establishment," Military Review, 42(9), September 1962, pp. 24-25.

Committee on Aeronautical and Space Sciences, Communication Satellites - Technical, Economic, and International Developments, U.S. Senate, 87th Congress, Sedond Session, Washington, D.C., 1962.

"Comsat Asks Inductry to Submit Proposals for Multi-Purpose Satellite able to Provide up to 6000 Two-Way Volice Circuits, or 10 TV Channels; Service Would Include TV Distribution, Air-Ground and Ship-Shore Links," Telecommunications Reports, (32) 4, 3, January 1966, pp. 1-2.

Corneretto, Alan, "60-Satellite Net Proposed for Military Communications," Electronic Design (10) 21, 11 October 1962, 8-11.

Cox, D. R., Renewal Theory, John Wiley and Sons, Inc., New York, New York, 1962.

Department of Defense Directive, 5160.50, 31 March 1964.

Dickieson, A. C., et al., Special Telstar Issue of Bell Laboratories Record, (41) 4, April 1963.

"Direct Broadcast Satellite for Home Reception," Electronics World, (75) 2 February 1966, p. 69.

Dorsey, J. S., "Defense Communications Satellite Program," Astronautics and Aerospace Engineering, (1) 8, September 1963, 52-53.

Dulles, Allen, New York, The Craft of Intelligence, The New American Library of World Literature, Inc., New York, New York, 1965, pp. 26-27.

Executive Order 11051, 27 September 1962, as amended.

Executive Order 10952, 20 July 1961, as amended.

Fischer, Laurins G., "Military Satellite Control," Astronautics and Aerospace Engineering, (1) 8, September 1963, 54-57.

Getler, Michael, "Planners Eye Comsats in the 1970's," Missiles and Rockets, (14) 24, 15 June 1964, 16-18.

Gerhart, N. R., Cause and Effect of Designating a DEFCON (Defense Condition) (U), FN-CN-100/000/00, Secret, System Development Corporation, 5 September 1962.

Headquarters North American Air Defense Command, Memorandum of Under-standing Concerning the Civilian Attack Warning System Between OCD and NORAD, Regulation 55-23, 30 November 1962, pp. 3-4.

Headquarters, North American Air Defense Command; Headquarters, Continental Air Defense Command, Operations, Defense Readiness Conditions, States of Alert, Alert Requirements and Air Defense Warning (U), NORAD/CONAD Regulation 55-3, Secret.

Headquarters USAF, Directorate of Operational Requirements, Deputy of Chief of Staff, Operationa, Tactical Warning Evaluation Study (U), Secret, Washington, D.C., 31 August 1962.

Holahaw, James, "Communications Satellites: The Technical Problems," Space/Aeronautics, (36) 3, September 1961, 112-121.

Holahaw, James and McDermott, J. R., "Advanced Syncom," Space/Aeronautics, (40) 4, September 1963, 79-88.

Hudson Institute, Strategic and Tactical Aspects of Civil Defense With Special Emphasis on Crisis Situations, Final Report, 7 January 1963.

Jaffee, Leonard, "NASA Communications Satellite Developments," Astronautics and Aerospace Engineering, (1) 8, September 1963, 48-51.

Joint Chiefs of Staff, Joint Operational Reporting System (U), Volume 1, Joint Chiefs of Staff, Pub. 6- 1 September 1963, Secret.

Kenworthy, E. W.; Lewis, Anthony; Frankel, May; "The Cuban Crisis: A Step-by-Step Review, New York Times, 3 November 1962.

Klass, P. J., "RCA, GE Study TV Broadcast Satellites," Aviation Week and Space Technology (84) 2, 11 January 1966, pp. 115, 117, 119.

Klass, P. J., "Support Grows for Airline VHF: Comsat" Aviation Week and Space Technology, (83) 21, 22 November 1965, pp. 83-86.

Lloyd, David K, and Lipow, Myron, Reliability: Management, Methods, and Mathematics, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1964.

Metzger, Sidney and Pickard, Robert H., "Relay," Astronautics and Aerospace Engineering, (1) 8, September 1963, 64-67.

Military Operations Subcommittee, Committee on Government Operations, Satellite Communications (Military-Civil Roles and Relationships), House of Representatives, 88th Congress, Second Session, Washington, D.C., 1964.

Miller, Berry, "Hughes Proposes TV Broadcast Satellite," Aviation Week and Space Technology, (82), 5, 1 February 1965, pp. 75, 77.

Norsell, Paul E., "Syncom," Astronautics and Aerospace Engineering, (1) 8, September 1963, 76-78.

Office of Civil Defense, OCD Warning Center Procedures for Operations of the National Warning System, OCD Manual 4305.1, January 1963, p. 1.

Office of Civil Defense, Realignment, Organization, and Responsibilities of the OCD National Warning System, Memorandum, 13 April 1965, pp. 1-2.

Office of the Federal Register, U.S. Government Organization Manual 1964-1965, Government Printing Office, Washington, D.C., 1 June 1964.

Parzen, Emanuel, Stochastic Processes, Holden-Day, Inc., San Francisco, California, 1964, pp. 276 ff.

Pierce, John R., "Communication Satellites," Scientific American, (205) 4, October 1961, 90-102, 204.

Powers, Patrick W., A Guide to National Defense, Frederick A. Praeger, Inc., New York, New York, 1964, pp. 33-34.

"Putting Space to Work to Educate the World," Business Week, 25 December 1965, p. 17.

Sandler, G. H., System Reliability Engineering, Prentice-Hall, Co., Englewood Cliffs, New Jersey, 1963.

Siegel, Lawrence, Radio Corporation of America, Letter to Henry Brown, Office of Civil Defense, Subject: Use of Satellite for Broadcasting Alerting Signals and Warning Information Directly to the Public, 6 October 1963.

Sorensen, Theodore C., Decision-Making in The White House, Columbia University Press, New York, New York, 1963, p. 10.

Stanford Research Institute, OCD Readiness - Readiness Indicator - Readiness Model, Draft, 5 February 1965, pp. 3, 4, 20, 21.

Stanford University, The Analysis of International Tensions: The Cuban Crisis of October 1962, 31 August 1963.

Stewart, Alsop and Bartlett, Charles, Saturday Evening Post, "In Time of Crisis," 8 December 1962, pp. 16.

System Development Corporation, Civil Defense Warning Requirements Study, TM-L-900/001/01, 31 January 1963.

Time Magazine, 30 April 1965, 85 (18), pp. 29-30.

Von Alven, William H., Ed., Reliability Engineering, Prentice-Hall, Inc., Englewood Cliffs, New Jersey, 1964.

Welber, Irwin, "Telstar," Astronautics and Aerospace Engineering, (1) 8, September 1963, 68-71.

APPENDIX B

GLOSSARY

Air Defense Emergency. Declaration of an emergency by the Commander-in-Chief-NORAD (CINCNORAD) indicating that hostile action is imminent or in progress.

Air Defense Warning. The degree of air raid probability. Warning RED: Attack imminent or in progress. Warning YELLOW: Attack probable. Warning WHITE: Attack improbable.

Air Raid Warning. A civil defense warning of probable or imminent attack by hostile forces.

Alert. The attention getting signal or alarm used to call the intended recipient to a state of action. An alert provides only an initial awareness of a threatening situation and does not in itself define that situation or the appropriate response to it. (See Warning.)

Alert Condition. A state of defense readiness within the civil defense system defined in terms of the degree of threat which exists at a given time and the type of actions taken by the system in response to the threat. (Also called CIVCON (Civil Defense Alert Condition).

Area Warning Circuit. That portion of the National Warning System (NAWAS) which is within one of the warning areas and connects the warning points of that area with a warning center.

Ballistic Missile Early Warning System (BMEWS) A real time, long range missile detection and tracking system under the operational control of NORAD which provide warning or missile attack against North America and the United Kingdom.

Bomb Alarm System (BAS) A network of sensors, transmission lines, and display equipment designed to detect the detonation of a nuclear weapon at selected locations within CONUS.

Clear Channel. A commercial AM broadcast channel on which the dominant station renders service over a wide area and which is cleared of objectionable interference within the primary service area of that station and over all (or a substantial portion) of the station's secondary service area.

Clear Channel Station. A commercial AM radio station that is assigned the use of a clear channel (q.v.).

Control Electromagnetic Radiation (CONELRAD.) A plan, now obsolete, to minimize the navigational aid that could be obtained by an enemy from continued operation of broadcast stations, to fulfill other national security requirements, and at

the same time, to provide for transmission of vital information to the public.

Defense Communications Agency (DCA) An agency within the Department of Defense charged with overseeing the design and operation of military communications systems.

Defense Readiness Condition (DEFCON) A state of readiness within the defense system of the United States defined in terms of the degree of threat which exists at a given time and the type of actions taken by the system in response to the threat.

Emergency Action Notification (EAN) System. Circuits and associated equipment designed to transmit an Emergency Action Notification message containing authorization to initiate emergency procedures to implement the Emergency Broadcast System plan.

Emergency Broadcast System (EBS) Those broadcasting stations and interconnecting facilities which have been authorized by the Federal Communications Commission to operate in a controlled manner during a war, threat of war, state of public peril or disaster, or other national emergency.

Emergency Operating Center (EOC) The protected facility in which governmental and civil defense officials having direct emergency responsibilities can safely carry on their emergency operations.

Ground Wave Transmission. Radio transmission via radio waves that are propagated over the earth and are ordinarily affected by the presence of the ground and the troposphere. Ground waves include all components of radio waves over the earth except ionospheric and tropospheric waves. Distinguish from skywave transmission (q.v.).

Industry Advisory Committee. One of the advisory committees to the Federal Communications Commission. Each committee is composed of representatives of the broadcasting industry at national (NIAC), regional (RIAC), state (SIAC), or local (LIAC) level. These committees assist the FCC in the execution of its responsibilities pursuant to the Executive Order that directs the creation of the Emergency Broadcast System.

Interdepartmental Radio Advisory Committee (IRAC) An independent agency which advises the FCC and the Director of Telecommunications Policy, Office of Emergency Planning on the planning, management, and use of radio frequencies by governmental agencies.

Key Station. An AM broadcast station (with a National Defense Emergency Authorization) linked to the Emergency Operating Center(s) of an area and capable of transmitting common program material over all NDEA station transmitters through an area program control network.

Local Industry Advisory Committee (LIAC) (See Industry Advisory Committee.)

Local Warning Center. A facility capable of 24-hour operation found normally at the city or county level. The local warning center must be capable of performing all functions required to provide warning to the inhabitants within its jurisdiction.

National Defense Emergency Authorization (NDEA) An authorization issued by the FCC permitting operation of a station as part of the Emergency Broadcast System during an emergency condition.

National Industry Advisory Committee (NIAC) (See Industry Advisory Committee.)

National Warning Center (NWC) The OCD facility staffed by Attack Warning Officers and situated within the Combat Operations Center at NORAD Headquarters. The NWC controls the NAWAS and activates the Emergency Broadcast System.

National Warning System (NAWAS) The federal portion of the Attack Warning System used for the dissemination of warning and other emergency information from OCD warning centers to warning points in each state.

North American Air Defense Command (NORAD) A coordinated defense of the North American continent against aerospace attack. The defense is coordinated between American and Canadian Services with full use of early-warning radar.

Random-orbit Satellite. A space vehicle that rotates about a planet, such as the earth, at a rate that differs from the rate of rotation of the planet and, therefore, is not always visible to a particular point on that planet. Several such satellites are required to cause the random probability that a satellite will be visible to any particular point on the planet to approach unity. A satellite in a random orbit about the earth is generally located at an altitude of from 100 to several thousand miles above the earth. (See Syncronons - orbit Satellite.)

Regional Industry Advisory Committee (RIAC) (See Industry Advisory Committee.)

Regional Warning Officer. A staff officer located at each OCD Regional Headquarters to assist states and local areas in solving warning problems.

Skywave Transmission. Radio transmission via radio waves that reach the receiving location after reflection from the ionosphere. Distinguished from groundwave transmission (q.v.).

Standing Operating Procedures (SOP) A fixed and approved method or procedure for accomplishing something.

State Industry Advisory Committee (SIAC) (See Industry Advisory Committee.)

Strategic Warning. A notification that enemy-initiated hostilities may be imminent.

Syncronons - orbit Satellite. A space vehicle that rotates in an equatorial orbit about a planet, such as the earth, at a rate equal to the rate of rotation of the planet. Because the rates of rotation are identical, the satellite appears to be stationary above a particular point on the surface of the planet. A satellite in a syncronons orbit about the earth would be located at an altitude of approximately 22,500 miles above the earth. (See Random-orbit Satellite.)

System. An assemblage of personnel, hardware components, and/or procedures functioning together in an orderly and prescribed manner to carry out a predetermined task.

Tactical Warning. A notification of enemy initiated hostilities.

Threat Warning. A report, originating at the NORAD Combat Operations Center, disseminating early warning information from DEW Line, Mid-Canada, and Pinetree Lines to lower echelons of the air defense system.

Warning. The advance notification of a nuclear threat, the effects of an attack, or impending natural disaster. Notification includes providing information about the nature of the threat, its extent or scope, its imminence, and the means by which to cope with it.

Warning Area. A geographical area consisting of a number of states which are the responsibility of one of the presently existing OCD warning centers.

Warning Point. A facility which receives warning and other emergency information over NAWAS and which relays this information according to instructions contained in state and local civil defense plans.

Washington Warning Area. The geographic area within a 20 mile radius from zero milestone, Washington, D.C., excepting that part of Howard and Ann Arundel Counties in Maryland falling within the 20 mile radius.

Washington Warning Area Control Point (WWACP) The location that controls the origination and/or dissemination of warning information to the Washington Warning Area. The WWACP also acts as an alternate to the National Warning Center in initiating the operation of the Emergency Broadcast System.

White House Communication Agency (WHCA) A subordinate agency of the Defense Communications Agency which provides all communications facilities for the President.

Unclassified
Security Classification

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY *(Corporate author)*

System Development Corporation
Santa Monica, California

2a. REPORT SECURITY CLASSIFICATION

Unclassified

2b. GROUP

3. REPORT TITLE

Final Report for the Office of Civil Defense, Civil Defense Warning System Research Support, Volume II: Research Studies

4. DESCRIPTIVE NOTES *(Type of report and inclusive dates)*

5. AUTHOR(S) *(First name, middle initial, last name)*

Special Research and Development Projects Staff

6. REPORT DATE	7a. TOTAL NO. OF PAGES	7b. NO. OF REFS
31 January 1966	202	56

8a. CONTRACT OR GRANT NO.	9a. ORIGINATOR'S REPORT NUMBER(S)
OCD-PS-64-183	TM(L)-1960/091/00
b. PROJECT NO. Work Unit Number 2212E	
c.	9b. OTHER REPORT NO(S) *(Any other numbers that may be assigned this report)*
d.	

10. DISTRIBUTION STATEMENT

This document has limited distribution and may be further distributed by any holder only with special approval of OCD Research.

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY

13. ABSTRACT

Summarizes the results of the research effort in the area of civil defense warning system and comprises the final report required by the contract.

DD FORM 1 NOV 65 1473

Unclassified
Security Classification

14. KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
OCD Civil Defense Warning System Research Support						