SAND77-0400
Unlimited Release

3151

Distribution
Category NRC-13

CONF-770656--20

A STRUCTURE FOR THE DECOMPOSITION OF SAFEGUARDS RESPONSIBILITIES

(Presented at the Eighteenth Annual Meeting of Nuclear Materials Management held June 28-30, 1977 in Washington, DC)

V. L. Dugan
L. D. Chapman

Prepared by Sandia Laboratories, Albuquerque, New Mexico 87115 and Livermore, California 94500 for the United States Nuclear Regulatory Commission under ERDA Contract AT(29-1)-789.

Printed August 1977

Sandia Laboratories

Nuclear Fuel Cycle Programs

DISCLAIMER

Issued by Sandia Laboratories, operated for the United States Energy Research and Development Administration by Sandia Corporation.

Printed in the United States of America
Available from
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Road
Springfield, VA 22161
Price: Printed Copy ~~$3.50~~ $4.00; Microfiche $3.00

SAND77-0400
Unlimited Release
Printed August 1977

Distribution
Category NRC-13

A STRUCTURE FOR THE DECOMPOSITION OF SAFEGUARDS RESPONSIBILITIES

V. L. Dugan
Systems Analysis Department 5740
and
L. D. Chapman
Systems Analysis Division I, 5741
Sandia Laboratories
Albuquerque, NM 87115

ABSTRACT

A major mission of safeguards is to protect against the use of nuclear materials by adversaries to harm society. A hierarchical structure of safeguards responsibilities and activities to assist in this mission is defined.

The structure begins with the definition of international or multi-national safeguards and continues through domestic, regional, and facility safeguards. The facility safeguards is decomposed into physical protection and material control responsibilities. In addition, in-transit safeguards systems are considered.

PREPARED FOR THE U.S. NUCLEAR REGULATORY COMMISSION
OFFICE OF NUCLEAR REGULATORY RESEARCH
UNDER ERDA CONTRACT NO. AT(29-1)-789

An approach to the definition of performance measures for a set of Generic Adversary Action Sequence Segments (GAASS) is illustrated. These GAASS's begin outside facility boundaries and terminate at some adversary objective which could lead to eventual safeguards risks and societal harm. Societal harm is primarily the result of an adversary who is successful in the theft of special nuclear material or in the sabotage of vital systems which results in the release of material *in situ*. With the facility safeguards system, GAASS's are defined in terms of authorized and unauthorized adversary access to materials and components, acquisition of material, unauthorized removal of material, and the compromise of vital components.

Each GAASS defines a set of "paths" (ordered set of physical protection components) and each component provides one or more physical protection "functions" (detection, assessment, communication, delay, neutralization). Functional performance is then developed based upon component design features, the environmental factors, and the adversary attributes. An example of this decomposition is presented.

Table of Contents

List of Figures

List of Tables

Introduction

A major mission of safeguards is to protect against the use of nuclear materials by adversaries to harm society. A structure for the decomposition of safeguards responsibilities and activities to assist in this mission will now be presented.

The structure begins by considering multi-national safeguards. This level of safeguards refers to safeguards exterior to national boundaries or exclusive of national boundaries. Domestic safeguards may be defined as being at and interior to national boundaries. Responsibilities in the U.S. would include the CIA, the FBI, the armed forces, and possibly other national response organizations. Regional safeguards responsibilities can be defined as being at and interior to regional boundaries. This regional responsibility might be a three or four state region, a state or a portion of a state. Local law enforcement agencies, the FBI, and the state police would have primary safeguards responsibilities within the region.

Facility safeguards can be defined at and interior to facility boundaries. The facility would bear the primary safeguards responsibilities with support from the regional authorities. In-transit safeguards can be thought of as the transport of material between facilities, between regions, or between national boundaries. Therefore, in-transit safeguards responsibilities must interact with multi-national, domestic, regional, and facility safeguards.

A further decomposition of facility safeguards responsibilities is the split of physical protection (PP) and material control (MC). Material control can be defined as being at and interior to the boundary immediately adjacent to material. Physical protection responsibilities encompass those safeguards issues exterior to the material boundary and up to the facility boundary. Under these definitions, material control includes

all safeguards responsibilities related to material accounting, material flow in a process line, and measures taken to delay or impede an adversary trying to directly acquire material. Physical protection encompasses responsibilities related to portal controls, alarms, barriers, security force responses, and communication systems. There is a strong interface between MC and PP. This interface is primarily at the access to a material location. Components at a glove box, such as detection components, may serve both as a MC and a PP component. An alarm from such a detection device may require MC to implement additional responses related to delaying material acquisition and also require PP to respond with a neutralizing security force or to deny exit of any employee until proper system behavior is restored.

Facility Characterization

A facility must be characterized in terms of an objective. In line with this objective the necessary personnel, procedures, and construction which allow the facility to operate and to accomplish this objective can be defined. Out of the definition of these items come the definitions of authorized locations of special nuclear material (SNM), authorized personnel and procedures for handling SNM, authorized vital equipment locations, and authorized personnel and procedures relative to vital equipment. The definition of these items of authorization forms the background for the application of facility protection systems. A protection system can do nothing more than see that all operations are in concert with procedures which have been duly authorized. Consequently, it is very important that the complete set of authorizations be reviewed by those responsible for the ultimate objective of the facility.

The first level of decomposition of the overall problem is that of authorized versus unauthorized adversary action. Although one thinks of any adversary action as being unauthorized, there are possibilities in which an adversary may obtain

an authorization. This would be classified as an authorized adversary action and will be discussed in more detail in a later section.

Adversary Attribute Definition

A set of adversary attributes must be defined so that the facility protection system can be evaluated. Typically, these adversary attributes are determined based upon an investigation of the level of protection provided by domestic, regional, and local safeguards resources. The adversary attributes against which the facility protection system must operate should be those which exterior safeguards structures are poorly suited to protect against. The exterior structures are particularly designed to protect against certain phases of adversary preparation, training, or collection of resources. Any attribute in one of these categories which has a small probability of being detected and consequently neutralized by a safeguards structure exterior to the facility becomes an attribute against which the facility must protect. This point can be illustrated by viewing the facility protection system as one element of a structure of safeguards systems which operate together to accomplish the overall objective of safeguards, which is to protect against the use of nuclear materials by adversaries to harm society.

Material stolen from a facility by an adversary intent upon constructing a nuclear weapon must be transported to a construction or storage location. Second, the adversary must construct the nuclear weapon. The third step would require the utilization of the weapon in situ or the transportation to another location prior to utilization. The ultimate utilization of this nuclear weapon by the adversary would then result in societal harm or risk. Prior to the effects on society, several safeguards responsibilities might interact to stop the adversary. These would probably include the PP and MC systems at the

facility prior to theft of the material, the regional, domestic and, possibly, the multi-national safeguards areas of responsibilities. Similar examples can be given related to the sabotage of a nuclear facility or the utilization of a weapon transported across national boundaries.

The Objective of a Facility Protection System

The outermost boundary of any nuclear fuel cycle facility defines a region of safeguards responsibilities. In other words, the responsibilities of the facility protection system exist at and interior to the outermost boundary of the facility. The objective of the facility protection system is twofold: first the facility protection system must protect against the theft of special nuclear material. In this context, theft refers to the removal of SNM beyond the boundary of the facility. Secondly, the facility protection system must protect against the release of radiotoxic material in situ. Any decomposition of the facility protection system into smaller areas of responsibility must be in line with these overall facility objectives.

Adversary Action Sequence Segment Definitions

Figure 1 indicates one way of decomposing the objectives of a facility protection system into smaller areas of responsibility. These smaller areas of responsibility may be designated as Generic Adversary Action Sequence Segments (GAASS). For each action segment the objective is to protect against the action which is described in the diagram in Figure 1. An an example, one subobjective would be to "protect against unauthorized adversary access to SNM locations." The key word in this first level of decomposition is authorized. An authorized action is any action which has been agreed upon by the facility operator and by the regulatory body to be necessary in accomplishing the objective of the facility's operation. We think of protecting against such action segments as "unauthorized adversary access

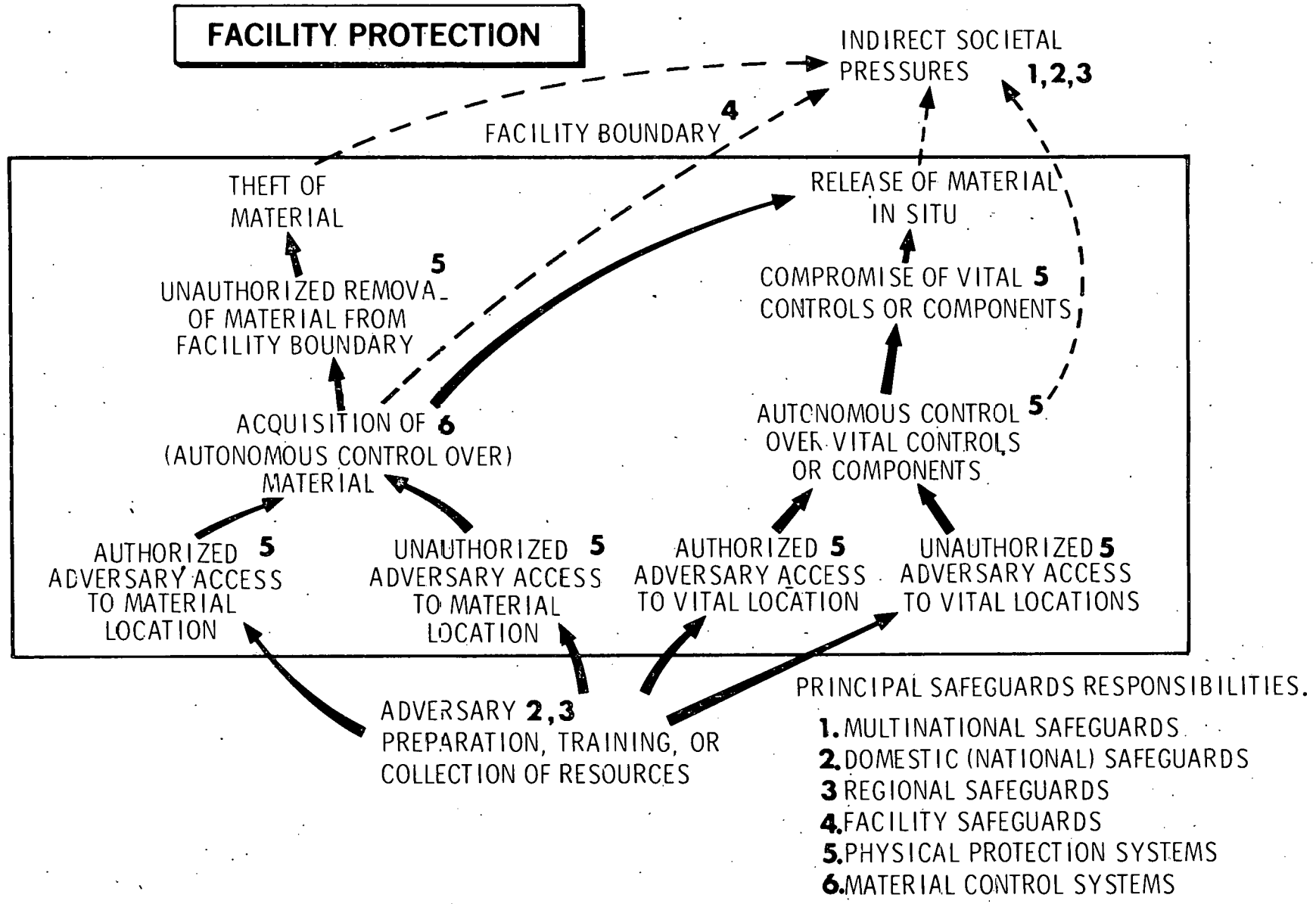

FIGURE 1. FACILITY PROTECTION

to SNM location or vital locations," or "unauthorized acquisition of materials," or "unauthorized removal of material from the facility boundary." In addition to the action segments which include the unauthorized, there are action segments which include the word authorized. Since there is the possibility that an adversary will actually be authorized to have access to SNM locations or to vital equipment or component locations, it is necessary to set up a structure which can also protect against this possibility. This structure is basically administrative and depends upon such items as employee background checks, employee testing, and employee reliability profiles that try to detect any possibility of an adversary being given an authorization. Each of the action sequence segments must be evaluated separately or in some combination to provide an adequate overview of the facility protection system performance against the defined spectrum of adversary attributes.

If a given generic adversary action sequence segment is selected, it then defines an initial point and a final point for adversary operations. Connecting the initial and terminal points of any action segment is a number of paths. A path may be defined as an ordered set of physical protection components with which the adversary or an adversary's materials must interface. In a realistic facility example there may be literally thousands of paths which may be defined with any given action segment. The performance of any of the components which make up the paths may be defined within one or more of the five functional classifications which follows:

Detection - To discover unauthorized acts by people or by hardware that may interact with people.

Assessment - To determine appropriate responses to detected unauthorized acts.

Communications - To notify appropriate response systems or forces of an unauthorized act or of the appropriate response to such an act.

Delay - To impede unauthorized actions.

Neutralization - To terminate an unauthorized act.

Evaluation of Paths

There are many random variables which actually determine the functional performance of any given physical protection system component. For any given component it is very difficult to describe its general performance in any one of the five categories by a single, complete model. Therefore, one must define a baseline performance under some assumed set of standard conditions and then define a set of abnormal conditions under which the entire system may be evaluated. The three primary types of conditions which are defined to aid in evaluating a given action segment are (1) site conditions, (2) environmental conditions, and (3) adversary action types of categories. All of these conditions essentially qualify or more explicitly define the ability of any given component to perform its function. Site conditions may include such things as normal operation, construction, maintenance, or emergency. Environmental conditions may include normal or abnormal weather or some other abnormal facility condition. Conditions on the categories of adversary action are of particular importance and are discussed in more detail in the next paragraph.

There are several categories of adversary actions which can be described. These categories of adversary actions are graphically outlined in Figure 2 and definitions for the various categories are given in the accompanying Table I.

The terms stealth and deceit are conditioning statements which apply to particular classes of detection components. The question of deceit arises at portals and other types of personnel or material checks where a falsification of authorized may take place. The word stealth describes covert action in abnormal

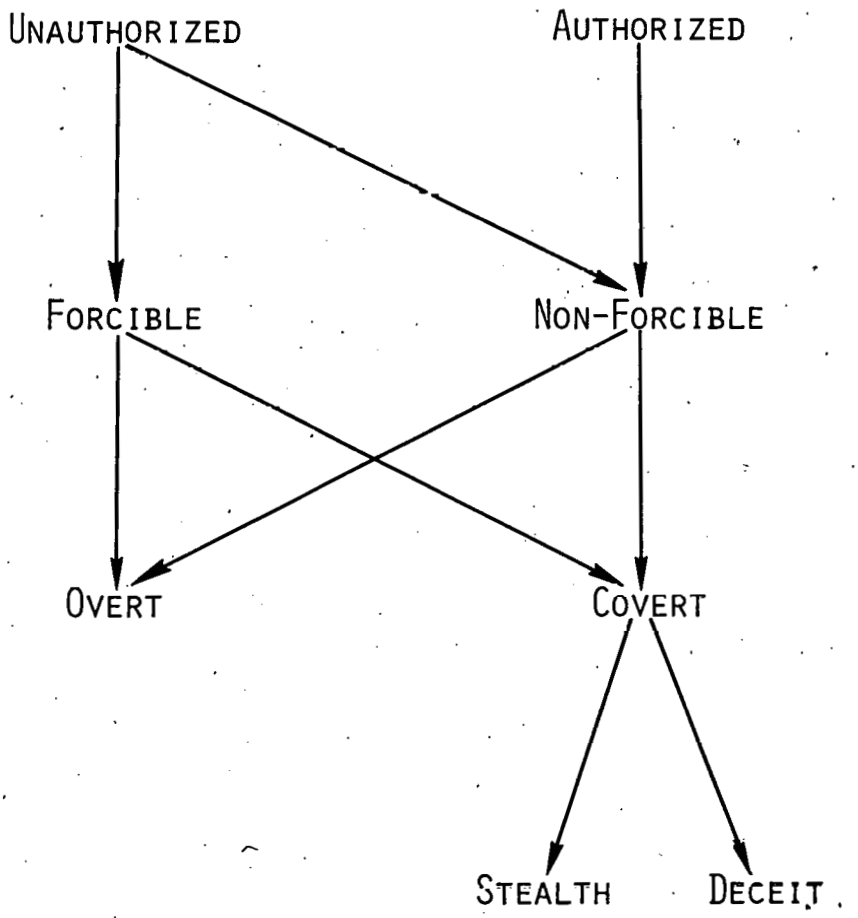

Figure 2

A Decomposition of the Categories
of Adversary Actions

(Arrows indicate possible combinations of the various categories of adversary actions within the several levels, e.g., a covert (stealth) non-forcible, unauthorized action.)

TABLE I

Definitions of Adversary Action Categories

Unauthorized - Any action which has not been defined by the facility operator or by the regulatory body to be necessary in accomplishing the objectives of the facility's operation.

Authorized - Any action which has been defined by the facility operator and by the regulatory body to be necessary in accomplishing the objectives of the facility's operation.

Forcible - An action in which a physical protection component is intentionally damaged or compromised.

Non-Forcible - An action in which no physical protection component is intentionally damaged or compromised.

Overt - Those actions in which the adversary does not attempt to avoid detection.

Covert - Those actions in which the adversary attempts to avoid detection.

Stealth - A type of covert action which takes place in abnormal channels, along abnormal or unauthorized paths, or under abnormal conditions.

Deceit - A type of covert action attempted in normal channels along authorized paths or under normal conditions by falsification of authorization.

circumstances and becomes a conditioning statement for the class of detection components used in the circumstances. Since both the words deceit and stealth describe the protection function of particular types of components, they are not necessary conditioning statements. A couple of examples will illustrate this point. An adversary attempting to gain access to a protected area using a counterfeit identification card would be acting in the mode of deceit. A card reader or a guard who is responsible for checking identification cards would be the component in the physical protection system designed to detect this particular type of adversary action. Therefore, a probability of detecting this type of adversary action could be assigned to the components which are designed for this particular detection function, and the descriptor of deceit would be unnecessary. In a like manner an intrusion alarm system on a perimeter barrier may be designed to detect entry along a certain portion of that barrier system. A covert entry along this barrier may be called stealth; however, the component placed at the barrier to detect this particular type of adversary action would be specifically designed for that purpose. Once again the word stealth is not a necessary conditioning term.

The lowest level of conditioning that must be given specific attention is that of overt versus covert. Since there can be transitions from overt to covert actions (or vice versa) at any point along an adversary's path, these conditioning terms are not easy to apply. The occurrence of these transitions is completely non-deterministic and is therefore very difficult to model unless a detailed simulation is used.

The next higher level of adversary action category, that of forcible versus non-forcible actions, has the same problems as that of overt versus covert. Once again the location or time of these transitions is non-deterministic; however, the performance of various components along an adversary path is extremely dependent upon this type of conditioning definition. This

difficulty may be handled in two ways. First of all, the conditioning descriptor may be imbedded in the definition of a component function of performance. As an example, detection and assessment probabilities could be based upon an assumption of covert actions and delay times could be based upon as assumption of overt accidents. These assumptions would provide a conservative, aggregate estimate of the physical protection system's performance. However, they could not be overly conservative or unrealistic. Secondly, the conditioning descriptors may be used to specify certain limits of performance for specific components for any given evaluation procedure. As an example, an evaluation may be done on a complete system assuming non-forcible adversary action. This would dictate a range of component performance for a given definition of adversary attributes. If the evaluation were repeated utilizing the conditioning assumption of forcible adversary action, the range of component performance for each of the five performance functions would change. The difficulty in repeating evaluations for large numbers of conditioning descriptors or statements is that a set of rules of performance must be generated for each evaluation. The larger the number of rules that are formulated, the more difficult is the final decision.

Another approach is to simulate the entire system and allow the performance of each component to be conditioned on a random basis. The application of Monte Carlo techniques to such a simulation allows the determination of a probability of system (or adversary) success under a range of possible conditioning factors.

Conclusions

An outline of a structure for the decomposition of safeguards responsibilities has been presented. This structure also lends itself to an evaluation of a facility protection

system utilizing today's evaluation techniques and, carried one step further, one could provide a means of illustrating the adequacy of a performance oriented assessment of facility protection systems.

DISTRIBUTION:

USNRC Distribution Section
Attn: Robert Wade
Washington, DC 20555
NRC-13 (208)

Vector Research, Inc.
Ann Arbor, Michigan
Attn: R. Blum

Atomic Industrial Forum, Inc.
7101 Wisconsin Avenue
Washington, DC 20014
Attn: Chris W. Hyvonen

Science Applications, Inc.
1200 Prospect St.
Box 2351
La Jolla, California 92038
Attn: Charles C. Schooler

Stanford Research Institute (2)
333 Ravenswood Avenue
Menlo Park, California 94025
Attn: Jacques Naar
Sigmund Scala

1000	G. A. Fowler Attn: D. B. Shuster, 1300
1310	A. A. Lieber Attn: W. Roherty
1700	O. E. Jones
1710	V. E. Blake
1712	J. W. Kane
1713	J. T. Risse
1714	E. I. Bruce
1715	W. D. Olson
1716	R. L. Wilde
1730	W. C. Myre
1750	J. E. Stiegler
1751	T. A. Sellers
1752	M. R. Madsen
1754	J. F. Ney
1758	T. J. Hoban, Jr.
4010	C. Winter
5000	A. Narath
5122	B. L. Hulme
5400	A. W. Snyder
5410	D. J. McCloskey
5412	J. W. Hickman
5412	G. B. Varnado
5412	D. E. Bennett

5700	James H. Scott
5740	V. L. Dugan (5)
5741	L. D. Chapman (25)
5741	K. G. Adams
5741	H. A. Bennett
5741	D. Engi
5741	L. M. Grady
5741	R. D. Jones
5741	M. T. Olascoaga
5741	D. W. Sasser
5741	A. A. Trujillo
8000	T. B. Cook, Jr.
	Attn: A. N. Blackwell, 8010
	L. Gutierrez, 8100
	C. H. DeSelm, 8200
	W. C. Schrivner, 8400
8300	B. F. Murphey
8320	T. S. Gold
8321	R. L. Rinne (5)
8360	J. F. Barham
8266	E. A. Aas
3141	C. A. Pepmueller (Actg.) (5)
3151	W. L. Garner (3)
	For ERDA/TIC (Unlimited Release)
3172-3	R. P. Campbell (25)
	For ERDA/TIC