Security Principles

FOR THE

PETROLEUM AND GAS INDUSTRIES

NATIONAL PETROLEUM COUNCIL

1625 K Street, N.W., Washington 6, D.C.

Walter S. Hallanan, *Chairman*
R. G. Follis, *Vice Chairman*
James V. Brown, *Secretary-Treasurer*

Petroleum Advisory Council to
DEPARTMENT OF THE INTERIOR
Washington 25, D.C.

Douglas McKay, *Secretary*
and
OFFICE OF OIL AND GAS
Hugh A. Stewart, *Director*

This Manual was prepared by a Task Force
of the Petroleum Administration for Defense

Published by the

National Petroleum Council

as a

Service to the Oil and Gas Industries, the Government, and All Others

Who May Find This Manual Helpful in Their Disaster Planning Programs

Security Principles

FOR THE

PETROLEUM AND GAS INDUSTRIES

May 5, 1955

Additional copies may be obtained
from Council headquarters
Single copies $1.00
Quantity prices on request.

TABLE OF CONTENTS

FOREWORD

In the preparation of this Guide careful consideration was given to the many pamphlets and reports which have been published by various Government agencies and private authorities on the subject of security protection of the petroleum and gas industries. This information has been reviewed and pertinent material has been incorporated into the text which may serve as a guide with respect to the elements, requirements and philosophy of security programs.

The prevention or winning of World War III may depend in considerable measure on effective industrial defense planning. It is self-evident that such planning must take place *before* attack. There will not be enough time after attack to carry out the amount and kind of planning and action that is required and "there's no miracle that can be substituted for time."

This is not to imply that a state of full industrial defense can be achieved overnight. On the contrary, only a start can be made now. Maximum readiness can only be achieved over the years, but speed in getting started is vital.

Part I

INTRODUCTION

A. DEFINITION OF "SECURITY"

"Security" as used in this document includes, but is not limited to, the adoption of measures and techniques to (1) minimize the loss of personnel, premises, processes and products or services due to industrial hazards, epidemics, or catastrophes caused by the elements; (2) prevent espionage and sabotage; (3) provide passive defense against enemy attack; and (4) expedite emergency restoration of productive or service capability in the Petroleum and Gas industries in both Peace and War.

B. IMPORTANCE OF PETROLEUM

It may be assumed that in the event of a third World War, it will be fought predominantly with the aid of petroleum, regardless of the potential uses to which the now unharnessed and apparently not readily available atomic energy is put. A modern Army, Navy and Air Force, as well as most of the Merchant Marine, are utterly dependent in their operations upon the petroleum product fueled engine which, depending upon the performance expected of it, may be reciprocating or jet propulsion in type. Vast quantities of special petroleum fuels (diesel oils for submarines; bunker oils for ships; high octane gasolines for conventional aircraft, P-T boats and tanks; special kerosene, fuel oil or gasoline blends for jet propelled aircraft and flame throwers), as well as enormous amounts of special lubricants, are required to serve the major units of the modern air, land, and sea armadas. In addition, recoil oils are required for field artillery and anti-aircraft pieces and machine guns; petroleum "jellies" for the most effective fire bombs; petroleum greases, oils and waxes for protecting equipment easily damaged by the slightest oxidation; special petroleum compounds for assuring sanitation and health; and other special petroleum compounds for accomplishing hundreds of other vital functions.

The Petroleum industry, besides providing those products associated with its name, produces the bulk of the nation's supply of toluene (basic component of TNT), and, furthermore, is one of the principle sources of butadiene and other components of synthetic rubber. Both toluene and synthetic rubber were predominantly "critical" items during World War II and reasonably may be expected to fall in the same category in a future war.

War is an all-out "total" effort in which military successes in the field bear a direct relationship to industrial productivity on the homefront. Not a wheel in industry can turn for long without lubrication. Essential automotive transportation, many railroads, and many components of industry are totally dependent upon petroleum for power. Heat, electricity and gas, so necessary to the health and essential needs of civilian war-workers, largely are dependent, either directly or indirectly, upon petroleum. Civilian needs, during total war, are inseparable parts of the total war effort.

The petroleum industry is highly integrated and interdependent. In effect it is comprised of a number of segments, its many operations including: (a) production, (the extraction of crude oils and gases from the earth); (b) refining, (the manufacture and processing of finished petroleum products from crude oil and gas); (c) transportation, (the movement by pipe line, tanker, barge, tankcar or tank truck of petroleum products from the oil fields to refineries, and from refineries to storage or distribution terminals or even direct to consumer); and (d) storage and distribution, (the storage and distribution of finished products at and from pipe line, river, seaboard, lakeside, and inland bulk terminals).

The petroleum industry, of all those considered extremely vital to our National existence, is unique for its extreme complexity. For example, interdependency of operations occurs not only within individual companies but often between separate and distinct companies. Although a single company and its subsidiaries often may operate integrated production, refining, transportation, storage, distribution and retail facilities throughout the entire country, other companies may engage in only one or a limited number of such operations and thus are dependent, in whole or in part, upon other operators for certain essential supplies or services. Refineries, sometimes located hundreds of miles from oil fields, are dependent upon pipe line, tanker, or tank-car facilities for supplies of base stocks. Similarly, bulk terminals, the storage and distribution facilities by which petroleum products are made available for off-shore or inland delivery to the armed services, essential industry, and domestic retail outlets, are dependent

upon petroleum transportation facilities for receipts of finished products from distant refineries. Transportation facilities, in turn, are dependent, on the one hand, upon the out-put of supplying oil fields or refineries and, on the other, upon the requirements and the storage capacities of refineries or bulk terminals receiving their throughput. All phases of the domestic petroleum industry are presently primarily dependent upon the production of crude oil and gas. Interdependency of operations is further reflected in the producing fields where, in a single field, dozens of companies independently engaged in production may use an integrated "gathering" system (a net-work of small pipe lines leading from wells or small storages to main storage) for collecting and storing their individual yields at the same "community" tank farm or the same common pipe line terminals from which their pooled production is pumped to refineries.

As another example of integration and interdependency of operations in the petroleum industry, a large portion of the country is covered with a net-work of trunk pipe lines which, in the case of "crude" lines, carry crude stocks from oil fields to refineries and, in the case of "products" lines, carry refined products from refineries to storage and distribution terminals or unfinished stocks to other refineries for further processing. These pipe lines, often extend over many states and connect many types of petroleum facilities. They fall into various categories operated as follows:

(1) By a "pipe line" company engaged solely as a common carrier for a number of individual oil producers or refiners:

(2) By a self-sufficient company whose pipe line activities represent only one operation in a series of related or wholly integrated petroleum operations;

(3) By a corporation formed from and controlled by the several different oil companies whose otherwise individual interests it serves;

(4) As a "system" of pipe lines comprised of, integrated with, and dependent for throughput on, any combination of the various types of operations mentioned in (1), (2), and (3).

For a considerable period during World War II, important refineries and storage and distribution terminals on the East Coast were dependent upon the integrated system of numerous connected pipe lines transporting petroleum supplies from remote oil fields and refineries. The dependency of refineries upon pipe lines and the dependency of pipe lines upon refineries and other pipe lines is common throughout the industry.

Because of this interdependency of operations, all phases of the complex petroleum industry must be furnished comprehensive over-all protection if production and safe delivery of finished petroleum products for national defense and other essential purposes are to be assured. It is not enough that the refining phase alone be protected.

Because of the integrated nature of the industry, comparative and complementary protection necessarily also must be afforded (a) truck pipe lines upon which vital refineries are dependent for supply and distribution of crude and refined products, respectively; (b) strategic storage and distribution facilities (particularly major pipe line, tank-car and tanker terminals) by which refined products are made conveniently available and in sufficient quantities to the armed forces and essential industries; and (c) oil fields (particularly high pressure fields where sabotage of one or two wells could damage an entire field) upon which remaining components of the petroleum and gas industries are dependent.

C. GAS

Gas is likewise vital to a modern industrial community. Gas may become a raw material in a manufacuring process and thus assume a special significance in certain specific cases, as numerous industries utilize gas extensively as a feed stock in their manufacturing operations. Of equal importance, gas has a wide domestic consumption. Gas facilities include production, transmission, storage and distribution systems supplying both natural or manufactured gas to wide areas. As a rule, these systems, unlike power facilities, are not generally interconnected. Consequently, destruction or damage to one of these facilities could curtail the gas supply in its area for all types of users. The industrial effect of disruption of a gas supply, considered together with its domestic uses, places gas facilities in the category of vital service facilities and makes their preservation a matter of concern to the national defense emergency effort.

Industries and domestic users have come to rely on the dependability of gas to meet their myriad and growing needs. It has always been the policy of this industry to develop ample capacity to meet critical demands, to provide the means for regular maintenance and emergency repairs, and to establish new facilities to serve the growing demand. During national defense emergencies, time, manpower, and materials may not be readily available to permit the gas industry to repair existing facilities or to create additional capacity through the construction of new facilities to meet the increased demands. It is, therefore, essential that gas systems be protected from damage to the maximum extent practicable.

Thousands of operations in commerce and industry, ranging all the way from the simple baking

of a loaf of bread to the smelting of steel in large furnaces producing hundreds of tons each day, attest to the universal importance of the modern gas industry. Between these limits we find gas used for commercial cooking and baking; for large volume water heating; in generation of steam in large boiler plants for industrial processes, electric generation and heating; for treating steel; in pulp and paper mills; brick, tile, cement, lime glass, carbon, sulphur, sugar, salt and chemical industries; as a raw-material in the manufacture of petrochemicals, a fast-growing industry; and in gas engines driving all kinds of machinery. This vital source of energy must be protected.

Part II

PURPOSE AND SCOPE

The primary purpose of this Guide is to provide uniformity, eliminate inconsistencies and furnish policy guidance for the establishment and administration of security programs throughout the petroleum and gas industries in the interest of National Defense.

This text is also intended to provide management with a basic guide in determining the scope and character of a security program and for formulating protective plans, methods and means which should be established to assure the continuity of product and service. Due to different system and facility characteristics, the degree of protection necessary for different systems and facilities varies so widely that no Guide of this kind could possibly provide specific recommendations applicable to all.

There is no simple solution to the problem of protection against the many forms of possible accidents, attack, subversive acts and sabotage; hence a protection program must be designed to fit each system and facility. Security is a continuing activity which must be expanded as hazards manifest themselves or are intensified.

The principles and guides for the development of security programs for petroleum and gas systems and facilities as set forth herein are applicable in some degree to all systems or facilities of the industry both large and small. In large systems and facilities, a security program may be greatly detailed involving many individuals, diversified functions and specific responsibilities. On the other hand, a small system or facility may find it practicable to combine a number of the applicable functions of such a program under a small number of individuals or even to repose the entire program in a single individual.

Part III

CONSIDERATIONS AS TO RISKS

As countries can actually be at war without a so-called "declaration of war" there is no schedule of time or events that can be considered as defining the end of a "cold war" and the beginning of a "shooting war." Terms are merely relative and are matters of degree. Therefore, estimates concerning the future cannot be used as a basis for rigid planning from which there is no deviation. An interim program may be devised, however, which will generally satisfy estimated future conditions. The measures suggested can be advanced or retarded to suit the actual situation, thus providing a considerable degree of flexibility.

Although we have the petroleum and natural gas background of World War II as a guide, there is no assurance that in the event of another war conditions will be comparable. The more time that intervenes between the last war and the next, the less assurance there will be that new emergency conditions, methods of attack, weapons of destruction, or means of protection, will be comparable.

However, for the guidance of the petroleum and gas industries, it may be assumed that the following conditions will prevail:

A. COLD WAR RISK

When international tensions exist, there is the risk of a full-scale war. Under such conditions, industry, with the advice of Government, should be reasonably prepared against espionage and against the contingency of a sudden outbreak of sabotage intended to reduce the war potential of the United States.

With respect to what may be expected from sabotage, espionage, and other clandestine activities in the United States, J. Edgar Hoover, Director of the Federal Bureau of Investigation, has advised that subversive activities today far exceed in seriousness any that we have previously had in this country. The subversive group is larger and more fanatical, and has better direction.

B. RISK IN EVENT OF FULL SCALE WAR

The United States has been fortunate in that no modern wars have been fought within its borders. Distance has provided a large measure of isolation which will continue to offer a measure of protection but may lead to a false sense of security. Difficulties of attack on this country are still great, but an aggressive enemy can bring war to our doors. Such an attack may come without warning. No part of the country is immune from bombing. From an enemy's strategic point of view, certain areas are more desirable for destruction than others, and each location requires study with regard to its vulnerability and importance to National security.

With respect to what may be expected from enemy air attack, it is quite possible that a considerable percentage of an enemy's bombers will be capable of penetrating our defense.

C. TIME ELEMENT IN SECURITY PLANNING

Since it is impossible to predict with any degree of accuracy when the tempo of a "cold war" may be stepped up to include widespread acts of sabotage or actual enemy attack, it is of prime importance that security plans covering such conditions be made so that they can be placed in effect without delay. Advance planning is imperative. Plans should be well formulated and understood by key employees so that no time will be lost when an emergency occurs.

The question of how far, under certain conditions, a given system or facility should go in the way of actual installation of barriers, personnel shelters, fencing, protective lighting, extensive use of guards, etc., is primarily a management decision. This decision should take into consideration the international situation, the character and importance of the requirements for continued operations, geographic location, economic and all other pertinent factors.

Part IV

FUNCTIONS OF GOVERNMENT

The Federal Government is responsible for the determination of the state of international conditions and relationships affecting the welfare and security of the Nation. In critical situations, the Government will issue such warning and take such action as may be prudent.

The Federal Agencies concerned with the field of internal security are many in number and divergent in duties. No one agency has sole and exclusive responsibility for the internal security of the United States.

Among these agencies are:

Atomic Energy Commission
Department of Agriculture
Department of Defense
Department of Justice
    Federal Bureau of Investigation
Department of Treasury
Federal Civil Defense Administration
Federal Communications Commission
Office of Defense Mobilization
U. S. Public Health Service

The functions of these Agencies are listed in the "U. S. Government Organization Manual," (28) *

* See Bibliography

Part V

FUNCTIONS OF INDUSTRY MANAGEMENT

It is the normal function of management to provide the facilities and operating organization required for a dependable supply of petroleum and gas. Under a national defense emergency this responsibility of management continues. However, the necessity of guarding against additional hazards that are not present in normal operation becomes an added responsibility.

Certain determinations must be made by management for such facilities as refineries; marine and inland pipeline terminals; oil pumpline pumping stations; compressor gas pipeline stations; gas regulating stations; pipeline river crossings; tank farms; distribution systems; research centers; natural gasoline plants and other facilities as appropriate. Because of its day to day operation of the facility, or system, management is in the best position to make the following determinations:

1. Organization for security emergency and disaster.

2. The level at which the protective program is to be maintained.

3. Selection of vital facilities.

4. The phasing of security measures.

5. The application of the graded protection and calculated risk principle.

6. The degree of compromise of security versus efficiency.

7. The determination and analysis of critical and vulnerable points in relative order, including process control and contamination.

8. The determination of the limits of compartmentation of information, dissemination or accessibility to documents, materials and areas.

9. Structural design, facility layout and site location of the facility, especially in reference to expansion and new construction.

10. Decentralization of facilities, supplies, personnel, vital equipment, utilities, water resources, etc.

11. Research and development for available substitutes to allow continued production in the event vital resources are denied or are in short supply.

12. Intensified repair and maintenance service for existing vital equipment.

13. Alternate sources of power, communications, utilities, water, materials, vital equipment and machinery, etc.

14. Evaluation and appraisal of security capabilities.

15. Responsibilities of security supervisory and operating agencies.

16. Evaluation of potential damage.

17. Employee and public relations.

18. Reduction of criticality and reduction of vulnerability.

19. Planning a protective program.

20. The extent of participation in a program for Civil Defense.

21. Availability of resources, including manpower, money, materials and time, which can be expended to provide security in competition with other demands of the facility or system.

Management should look to responsible governmental authority for advice as to the nature, extent, and degree of imminence, of hazards that may be present in periods of national defense emergency.

Part VI

SELECTION OF VITAL FACILITIES

A. CRITICALITY AND VULNERABILITY

In order for management to assume its responsibility for the protection of the system or facility it must first evaluate its systems or facilities. All systems or facilities occupy a place in the national defense economy which will contribute to a greater or lesser degree to the Nation's ability to fight. Therefore, the loss of any system or facility, material or personnel, is to some degree a detriment to the national defense potential. On the other hand, security protection programs consume manpower and materials which in times of emergency are in short supply and, therefore, must be utilized to the greatest possible advantage. Since it is not economically possible or theoretically necessary that facilities of every kind and character achieve the same degree of protection, the determination of the degree of protection warranted in any particular system or facility is predicated upon an analysis of two factors, (1) relative criticality and (2) relative vulnerability.

The term, relative criticality, is used to describe the relative importance of a portion of a facility or system to insure continuity of production or service. The portion of the system or facility which is considered to be of high criticality is one whose partial or complete loss would have an immediate and serious impact on the ability of the system or facility to provide continuity of production or service for a considerable period of time. The criticality of a portion or part of a system or facility may bear no direct relationship to its size or whether it produces an end product. Management is fully familiar with the widespread curtailment of production or service resulting from the loss of a relatively small part of a facility. Hence, criticality must be determined upon the basis of the portion or part of the facility to the whole system or facility as a unit.

In determining relative vulnerability, management must determine the susceptability to damage of each part of its system or facility and the means by which the portion or part of the facility may be damaged. A portion or part of a facility or system may be critical but not vulnerable. A portion or part of a facility or system may be vulnerable but not critical.

The degree of graded protection afforded to the portion or part of the system or facility is determined by the relationship of relative criticality and relative vulnerability. A system or facility which is both highly critical and highly vulnerable is the ideal target for enemy action. Hence, an extensive security protection program becomes a necessity for those portions or parts of a system or facility which are both highly critical and highly vulnerable.

Relative criticality and vulnerability considerations should be given to facilities, such as short supply components (benzene, codimer, tetraethyl fluid), water and power supply; high pressure wells, key pumping and compressor stations upon which the continuous operation of the oil and gas pipeline system depends; strategic river and other water crossings, whose destruction would be as disastrous as the loss of a key pumping or compressor station; originating, intermediate and terminal stations upon which continuous operation of the system is dependent; important interconnections with other pipe lines and other components.

On the basis of known experience of other wars, the enemy will seek out petroleum and gas areas for destruction. His goals or targets will be vital refineries, transportation facilities, pressure regulation stations, storage and distribution terminals, recycling and natural gasoline plants and major oil and gas fields. To determine which facilities or systems will continue to warrant protective measures, a continued evaluation should be conducted of all vital components of the complex, interdependent petroleum and natural gas industries. Re-evaluation should be made periodically according to world conditions but, in any event, at least annually.

B. CRITERIA FOR SELECTION

From the application of the foregoing criteria, and from a determination of the guiding factors outlined later for specific types of petroleum and gas facilities, individual facilities or portions of facilities should be assigned identifying criticality and vulnerability ratings. Among other things, these ratings must take into consideration the products or services which are of highest importance to national defense and for which there is a shortage or near shortage of supply and no suitable substitute.

Oil and gas producing, refining, transportation, storage and distribution facilities all play their own individual but inter-related roles in bringing about the desired end result—the adequate supply and availability of gas and refined petrolem products without which modern nations cannot maintain themselves either in war or in peace. In determining which of the various component facilities are predominantly important links in the chain of ultimate supply and delivery, and thus of primary importance to the prosecution of a war, appropriate consideration should be given to their integration and interdependency. In addition, the following major criteria should apply to each individual facility evaluated:

a. Importance to the national defense of the product furnished or the service rendered by such facility.

b. The relationship between the available supply of the product or service to military and essential civilian requirements.

c. The inherent dangers involved in the production, manufacture, transportation, storage or distribution of a product or in the furnishing of a service.

C. GUIDING FACTORS

The guiding factors to be given specific consideration evaluating the various types of petroleum and gas facilities are as follows:

1. FOR REFINERIES:

a. Normal and potential crude oil capacity.

b. Normal and potential out-put of specific war-important products (such as high octane aviation gasoline, toluene; butadiene, and vital components thereof).

c. Number of vital and difficult-to-replace catalytic, polymerization, hydrogenation or alkylation units in operation—and comparison of this number against the total of such units in this country.

d. Replacement time.

e. Normal and alternate supply sources of crude requirements.

f. Strategic location.

2. FOR PIPE LINES:

a. If a crude line, determination as to whether the pipe line under review is either a major outlet for a producing area (i. e., oil fields) or is a truck line connection serving as a major source of supply for specific refineries or refining districts.

b. If a products line, determination as to whether the pipe line is a major outlet for specific refineries or a major source of supply for terminal areas supplying the armed services, essential industrial and domestic outlets, or seagoing tankers.

c. If a gas line, determination as to whether the pipe line under review is either a major outlet for producing area or a trunk line connection serving as a major source of supply for specific communities.

d. Throughput capacity.

e. Replacement time.

f. Normal and alternate sources of supply.

3. FOR TERMINALS:

a. Storage capacity.

b. Normal and potential throughput.

c. Kinds and quantities of products stored or distributed.

d. Value as a distribution facility to the armed services, essential industry, essential civilian outlets, and overseas transportation.

e. Strategic location.

f. Replacement time.

4. FOR OIL AND GAS FIELDS:

a. Normal and potential production.

b. Estimated underground reserves.

c. Kinds and quantities of gas or special crudes produced.

d. Whether a high or low pressure area.

e. If a high pressure field, proximity to industrial and/or military establishments, or highly important maritime operations which might be endangered if a well or wells were to go out of control.

f. Pipe line outlets for transporting crude to refineries.

5. OTHER PETROLEUM FACILITIES:

Natural gasoline and re-cycling plants generally are associated with either the refining or the oil and gas field phase of the petroleum industry, but sometimes are of sufficient individual importance to warrant ratings in their own right. Similarly, compounding plants and research laboratories, although often integral components of refineries, also may warrant individual ratings.

6. GAS FACILITIES

Gas facilities should be evaluated as to relative criticality upon the basis of the following criteria:

a. Relative to the community and importance to military and industrial installations served.

b. Ratings based upon community consumption should consider:

(1) The size of the community and the degree of dependence upon gas for essential private and public function.

(2) The proportion and importance of the industrial consumption as compared with domestic consumption.

(3) The proportion of national defense industries' consumption to total industrial consumption.

(4) The emergency potential quantity of standby fuels or energy available for national defense industries through inter-connections of power plants and power systems.

(5) Replacement or repair time.

c. Relative criticality ratings based upon industrial and military installation consumption should consider:

(1) The present or potential importance of the industrial or military installation and the degree of its dependence upon gas for operations.

(2) The surplus capacity and supply reserve available to the installation in emergencies through reduction of non-essential consumption, available auxiliary gas plants, gas storage facilities, standby fuels, or inter-connections.

(3) Hazards created by interruption of service.

(4) Replacement or repair time.

d. The effect that the loss of the particular portion or part of the system or facility would have on the production capacity of the installation served by the system or facility.

In general, the most appropriate procedure in evaluating various components of the petroleum and gas industries is to evaluate refineries first, transportation facilities, then terminals, and last producing fields. Thus, correlated information, often of contingent value in evaluating the several phases of the industries, automatically is built up in its proper sequence as the over-all evaluation continues.

Part VII

HAZARDS

Having determined the critical and vulnerable portions of the system or facility, management must determine the probability of damage to these portions or parts of a system or facility from:

A. Hazards inherent in the production or service operation.

B. Espionage.

C. Sabotage.

D. Direct Enemy Attack.

These hazards have been listed in the order in which they are most likely to occur.

A. HAZARDS INHERENT IN PRODUCTION OR SERVICE OPERATION

A protective program is not confined to meeting the most hazardous situations; it is a continuing activity beginning in peacetime and expanding to meet the particular hazards of formal hostilities. Increased production for national defense emergency naturally intensifies routine hazards. Specific hazards to the petroleum and gas industries depend on such variables as industrial process, the type of facility, facility layout and construction, the level of the organized protection and prevention program enforced by management, location, topography, climate, etc.

Management must be alert to recognize increased risks and must correspondingly increase protective and preventive measures. Management, as part of its normal operation, is aware of the protective measures necessary for dealing with hazards inherent in production and service operations. Private organizations such as the American Petroleum Institute, American Gas Association, the National Fire Protection Association and others have issued information pertaining to these hazards.

B. ESPIONAGE

Espionage includes the collection of information which contributes to an evaluation of the Nation's war potential and which may be used to advantage by an enemy in subversive activities and armed force attack. The very nature of the petroleum and gas industries makes it difficult to conceal many phases of its operations. In spite of this, it is desirable that these industries use discretion during a period of national emergency in the release of information that might be useful to the enemy, even though such information may already be considered common knowledge. The enemy will not risk trained men, expensive equipment and costly munitions unless the destruction of the targets selected will appreciably decrease our ability to wage war. The enemy will be continuously endeavoring, long prior to an actual armed attack, to ascertain where and what these targets are. He will further endeavor continuously after the initial attack to obtain the same information in order to mount additional attacks.

All system and facility personnel, generally, are acquainted with the type of espionage carried on by professional spy rings. Such espionage, while glamourous and effective for limited purposes, does not produce for a potential enemy the vast mass of detailed, accurate information concerning the vital petroleum and gas facilities of this country which is necessary to destroy systematically our production method. These data may already be developed piecemeal through contributions of many agents whose fragmentary reports fit together like pieces of a jigsaw puzzle to complete a precise picture of the petroleum and gas industries and civilian war structure.

Espionage agents specifically seek information such as the following:

(1) Capacity, rate of production, industrial mobilization schedules, and details of orders on hand.

(2) Specifications of products.

(3) Test records of newly developed items or equipment.

(4) Sources of raw materials and components.

(5) Destination of completed products and transportation routes.

(6) Data on production methods.

(7) Critical points and possible methods of effective sabotage.

(8) Measures in force for security and to prevent sabotage, such as, frequency of inspection by guards and their dependability.

(9) Names of dissatisfied employees and non-employees who might be susceptible and utilized for subversive plans.

Espionage agents may be expected to use great ingenuity in obtaining information by:

(1) Infiltrating into plants as employees, visitors, inspectors, or by other means.

(2) Obtaining information from employees by (a) stealing, (b) purchasing, or (c) encouraging them to "talk shop."

(3) Stealing information from records or other sources and reporting personal observations and studies of production operations, test runs or classified materials.

(4) Using various means of reproducing documents, products, processes, equipment, or working models.

(5) Using "fronts," such as commercial concerns, travel agencies, import-export associations, scientific organizations, insurance agencies, businessmen's groups, and other organizations to obtain confidential information or pertinent statistical information which can be translated into strategic information.

(6) Using threats of danger to friends or relatives of an employee, to obtain information.

(7) Using blackmail techniques by threatening to expose intimate and personal details concerning an individual.

(8) Skillful extraction of information from members of the family or close friends of an employee.

(9) Picking up information at social gatherings.

(10) Personal observation of production operations, test runs, shipment of finished product or confidential papers.

(11) Securing information from waste and carbon paper and other discarded records.

(12) Increasing the susceptibility to recruitment for the cause by playing on the emotions such as love, hatred, desire for power, etc.

The following will serve as an example of the range of information covered in a report on a petroleum products pipe line system compiled by a professional espionage organization from data received from miscellaneous sources:

(1) OWNERSHIP:

a. Government, (central department or departments).

b. Private (with affiliations).

c. Joint

d. Policies and regulations governing construction, operations, maintenance and traffic.

(2) ADMINISTRATION:

a. Organizational levels of responsibility.

b. Personnel directing operations, maintenance and traffic.

c. Personnel requirements for operations and maintenance.

d. Personnel morale and discipline, wages, hours, efficiency, availability (skilled or unskilled) organization, centers of recruitment and location.

e. Military consideration.

(3) GEOGRAPHIC:

a. Physical characteristics of country traversed.

b. Extent and location of system.

c. Junctions.

d. Port and rail outlets.

e. Under and over water sections.

f. Critical and vulnerable points, and possible methods of inherent sabotage.

g. Strategic importance.

h. Construction, rehabilitation and operations, new, planned and proposed.

i. Construction and operational continuity, limitations.

(4) PIPE-LINE DATA:

a. Commodity carried.

b. Number of lines and diameter and weight of each.

c. Volume of flow (liquid or cubic measure, shown in both English and metric terms).

d. Pressure under which operating.

e. Covering or insulation on pipe.

f. Temperature of line.

g. Buried or open with depth buried if known.

h. Specific area traversed by line with distances between major or intermediate terminal points.

i. General condition of line (old—new) including dates of construction and rehabilitation.

j. Principal customers served.

k. Type of communications system owned or used.

(5) PIPE-LINE CONTINGENT STRUCTURES:

a. Location.

b. Type, construction and size.

(*a*) Bridges, trestles and underwater crossings:

Length of span; height above and below ground —water, number pipe carried; wood, steel or concrete.

(*b*) Stations:

Area; number of booster stations in each pipeline unit; type of structure; number of pumps; products named, throughput capacity of each, total for each station; fuel; and fire protection.

(*c*) Storage facilities:

Number tanks serving each pipeline unit and

apart from separate storage installations; size tanks, capacity; above or below ground; fire protection.

(*d*) Power lines and facilities.

(*e*) Repair, maintenance facilities, and stocks,

c. Maintenance labor: number of workers, type and source.

(6) Procurement:

a. Purchase of pipe.

b. Purchase of motors, engines, pumps and compressors.

c. Purchase of work equipment.

d. Purchase of building equipment.

(7) Security measures and susceptible employees or non-employees.

(8) Assigned priority for destruction or interruption.

(9) Detailed plan for disruption or interruption.

(10) Additional detailed information requirements.

(11) Supervisory assignment.

GENERAL:

In general, espionage may be rendered ineffective or made more difficult by the application of protective measures such as, a careful loyalty check of personnel, particularly, before employment, prevention of unauthorized entry to the premises; special guarding and handling of classified material; restriction of movement within the system or facility; and security education and training of employees and others who have information on the system or facility's activities.

C. SABOTAGE

Industrial sabotage is the most effective method that can be applied against a national defense emergency effort. The fact that very little damage in the last war was directly traceable to enemy sabotage might well be attributed to the lack of ingenuity exercised by the enemy in the direction of sabotage and the selection of sabotage methods rather than to his failure to appreciate the necessity of this form of warfare. Industrial sabotage is a basic doctrine of the Communist party and other revolutionary bodies. The undeniable existence of this doctrine, the highly effective results which may be accomplished by the skillful employment of sabotage, and the known existence of substantial groups within this country available and willing to undertake such work places this hazard higher upon the list of risks confronted by our industry than at any time in the history of this country.

In terms of trained manpower, equipment, and munitions risked, a sabotage operation involves only negligible expenditure by the enemy, but the profit may be enormous if the target has been strategically selected. The disastrous consequences of an act of sabotage, such as the destruction of a critical refinery, may be grossly disproportionate to the manpower, time, or material devoted to the act. It is only realistic, therefore, to assume that the outbreak of a formal attack on this country may be accompanied by one or a series of well planned major sabotage efforts. In addition, however, throughout the period prior to the initial formal attack and thereafter, tremendous loss may be occasioned by a multitude of small acts whose cumulative effect may be greater significance than an initial or subsequent major sabotage plan.

1. METHODS

The tools and methods of sabotage are limited only by the skill and ingenuity of the saboteur. A major sabotage effort may be undertaken after thorough study of the physical layout of the petroleum and gas system or facility and its production processes by technical personnel fully qualified to select the most effective vehicle to strike one or more of the most vulnerable parts of the system or facility. Sabotage may, on the other hand, be improvised by the saboteur relying solely upon his own knowledge of the system or facility and the materials available to him. The petroleum and gas industries are well aware of the inherent sabotage possibilities to them through the use of products available in the normal facility operation of the industries themselves. An example of this is the sometime availability on the site of explosives intended for industrial purposes, product and process contamination by the use of additives and spoilers, incorrect cycle time phasing, tampering with control devices, operating equipment, etc. The saboteur, in such a case, may or may not possess or need a high degree of technical knowledge. Hence, the device or agent selected for sabotage may range from the crude or elementary to the ingenious or scientific. The methods of sabotage may be generally classified as follows:

(a) Mechanical—breakage, insertion of abrasives and other foreign bodies, failure to lubricate, maintain and repair, omission of parts.

(b) Chemical—the insertion or addition of destructive, damaging or polluting chemicals in supplies, raw materials, equipment, product or utility systems.

(c) Explosive—damage or destruction by explosive devices or the detonation of explosive raw materials or supplies.

(d) Fire—ordinary means of arson, including the use of incendiary devices, ignited by mechanical, chemical, electric or electronic means.

(e) Electric and Electronic—interfering with or interrupting power, jamming communications, interfering with electric and electronic processes.

(f) Psychological—the fomentation of strikes, jurisdictional disputes, boycotts, unrest, personal animosities, inducing excessive spoilage and inferior work, causing "slow-down" of operations, provocation of fear or work-stoppage by false alarms, character assassination; on a larger scale, the instigation of false political and economic public issues and the dissemination of inflammatory propaganda so as to break morale.

2. OBJECTIVES

The objectives of the saboteur in a particular system or facility may include one or more of the following:

(a) Damaging buildings and equipment.

(b) Damaging power, communications, water and sanitation systems.

(c) Tampering with testing devices.

(d) Tampering with drawings and formulae.

(e) Infecting or polluting water and foodstuffs.

(f) Tampering with ventilating systems or polluting the air supply.

(g) Tampering with personnel safety devices and equipment and otherwise creating conditions which would injure personnel.

(h) Damaging, spoiling, or destroying the product of the plant.

(i) Sabotaging manpower by use of psychological methods discussed above.

A definite distinction must be made, however, between manpower sabotage by psychological means, such as the fomentation of strikes, "slowdowns," and the like, and legitimate labor activities. Manpower sabotage of this nature is extremely difficult to detect. One disloyal employee engaged in psychological sabotage may influence others who will thereupon, believing in good faith that a labor grievance exists, engage in strikes and other activities resulting in loss of production.

Panic may be a far greater threat to the national emergency defense effort than any other weapon, including the atomic bomb. As a weapon, it may be used to our detriment. Panic is the result of fear and unreasoning fear is usually the result of insufficient knowledge or lack of confidence in leadership. Psychological defense may be achieved in three major steps: (1) preparation, (2) collection and dissemination of information, (3) action. It is the building and maintaining of morale; informing employees of threatened dangers, how they may be recognized, what protective measures are available and what defense should be utilized that counts. Employees must have faith in these measures themselves, and in the company leadership.

The saboteur is not necessarily a foreign national or of foreign parentage. He may be a highly trained professional or rank amateur. He may be a laborer, a machinist, a foreman, a top-flight engineer, or even a member of management. He may be anyone. But one thing is certain—he is likely to be one of the least-suspected members of the organization.

His motives may be as varied as his personality. He may work for love for his native land; for pay; for hatred; for sincere, if misguided, devotion to a cause; for revenge; to settle a real or imaginary grievance; or under threat of blackmail or fear of reprisal against relatives in the enemy country.

Physical sabotage is essentially an inside job, or requires the assistance, knowingly or unknowingly, of someone inside.

Hence, the principle protective measures must be designed to limit the entry or continued presence of saboteurs or his assistants.

D. DIRECT ENEMY ATTACK

At the immediate outset of any future war and continuously thereafter it is certain that in addition to sabotage, the enemy will attack the vital petroleum and gas systems and facilities of this country with the most effective weapons available to him. Obviously, the responsibility for preventing or minimizing such direct attack rests primarily with the Armed Forces. While the system or facility personnel cannot know in advance the nature or capabilities of the enemy's striking force for this type of attack, it is reasonable to anticipate that such attack may proceed initially or from time to time after the outbreak of the war along any of the following possible lines:

a. Air attack.

b. Chemical attack.

c. Biological warfare.

1. AIR ATTACK

Although many of the points listed below are controversial, it may be said that:

(a) Major refinery units are easily damaged.

(b) In no case, with the possible exception of the atomic bomb, will complete destruction of a refinery be accomplished regardless of the weight of the attack or attacks.

(c) Petroleum pipe lines and tankage, although easily damaged, are quickly replaced or by-passed and, hence, do not materially affect production.

(d) Continuity of production or service may be more easily reduced by attacking outside sources of the system or facility such as, power, water, etc.

(e) Attack by fragmentation bombs on high pressure systems containing inflammables, followed by an attack of incendiaries, will result in considerable damage.

(f) Trained fire-fighting crews and adequate equipment in refineries can materially reduce damage.

(g) Personnel casualties can be held to a minimum with personnel shelters.

(h) Blast walls of steel, concrete, or earth may reduce damage to equipment and tankage from near misses of 500-lb. bombs and under.

(i) Smoke screens, camouflage, and decoy plants are only sporadically effective.

(j) Except for units producing certain specialty items, construction of underground refineries should not be attempted.

(k) Refineries constructed underground will, in all probability, have to rely on outside sources of supplies, power, water, etc.

(l) An adequate warning system will enable the facility to continue its production or service with as little interruption as possible.

(m) Plans should be made for provision of personal shelters for personnel that must remain on duty regardless of hazard.

(n) First-aid training.

The petroleum and gas industries must be prepared to provide protective measures to minimize the effects of atomic, high explosive, incendiary, bacteriological or biological, chemical or radiological attacks. The primary problem in the event of such an attack is to determine which disaster measures are to be undertaken by the system or facility personnel.

a. Atomic and Radiological

The following summary is drawn from the report entitled "The Effects of Atomic Weapons," published in August 1950, and available from the Superintendent of Documents, U. S. Government Printing Office, Washington 25, D. C. (Price $1.25). This information is based on the effects of an atomic bomb similar to those dropped on Nagasaki and Hiroshima, which were equivalent to 20,000 tons of TNT with an air burst at 2,000 feet. More efficient atomic bombs and other nuclear devices have since been developed, but for the purpose of this text the following will suffice:

(1) Virtually complete destruction will occur out to a radius of approximately one-half mile from ground zero, corresponding to an area of destruction of about three-quarters of a square mile. Eighty-five percent mortality will occur in this area.

(2) Severe damage, defined as major structural damage that would result in collapse or liability to collapse of all buildings, except those of concrete and heavy steel frame, will occur out to a radial distance slightly in excess of one mile from ground zero. This corresponds to an area of four square miles in which the damage ranges from severe to destructive. Thirty percent mortality will occur in this area.

(3) Moderate damage, short of major structural damage but sufficient to render the structure unusable until repaired, will occur out to a radius of about one and five-eighth miles, and most old style brick and frame buildings will be seriously damaged, giving an area of eight square miles in which the damage ranges from moderate to destructive.

(4) Partial damage will be inflicted out to a radius of approximately two miles, adding four additional square miles to damaged area, and making a total of 12 square miles subject to some degree of damage in excess of plaster damage and window destruction.

(5) Light damage, which is mostly plaster damage and window breakage, may extend out to a radius of eight miles or more, giving a light damage area of about 200 square miles. Actually these distances, at which window and light plaster damage will be inflicted, vary appreciably with the meteorological conditions at the time of the detonation and may be considerably greater under conditions which provide a temperature inversion in the lower atmosphere.

All categories of damage will vary with topographical and meteorological conditions. The shock wave that moves out is the most destructive result of an air burst. Starting behind the shock wave, but soon passing it, are the waves of thermal radiation which travel with the speed of light. The thermal wave lasts about three seconds, is intense enough to start primary fires in combustible materials for approximately one mile, and it is estimated that primary and secondary fires will probably cause about 20 to 30 percent of the total fatalities.

For a more complete discussion of thermal radiation effects, see Chapter "C", pages 196 to 211 of the "Effects of Atomic Weapons."

Four types of radiation result from the explosion of an atomic bomb: gamma rays, neutrons, beta particles, and alpha particles. Gamma rays and neutrons constitute the important initial ionizing radiation. Unlike the heat flash, the gamma rays have great penetrating power. The lethal range of the gamma ray is approximately 4,000 feet. Neutrons have a shorter lethal range and less penetrating power and do not provide a significant extra hazard. They may cause slight induced radioactivity.

The induced radioactivity consists principally of gamma and beta radiation. In an air burst of more than 500 feet above ground the residual radiation on the ground will be negligible.

The total radioactivity is very large at the instant of an explosion. It decays rapidly. At the end of one hour it is only 1/130 of the first minute. The

explosion produces many radioactive elements whose half-lives are from a fraction of a second to thousands of years.

The effect of ionizing radiation on humans is in proportion to dosage measured in roentgens. It is generally accepted that 400 roentgens received over the whole human body within a few minutes will be lethal to about 50 percent of human beings.

In the event of an underground or underwater burst a considerable amount of induced radioactive material will be thrown into the air and fall out on the surrounding area creating a potential serious hazard.

Radiological warfare might be conducted by the use of radioactive materials obtained and distributed otherwise than by atomic bomb explosions.

The radioactive materials can be obtained by controlled fission in a reactor as a by-product in atom bomb material manufacture or by exposing certain materials to neutron bombardment in a reactor. It is not easy to produce sufficient quantities of radioactive materials for waging radiological warfare and most of them cannot be stockpiled for very long periods, because they decay continuously.

It is difficult to lay down enough radioactive material to cause serious injury by a short exposure, but if effective quantities were laid down secretly, considerable injury might be caused before the act was detected.

Perhaps the most important use of radioactive materials as a weapon is for panic, annoyance, and morale reducing purposes. The threat of use, or actual use even on a small scale, would cause diversion of effort, alarm, and even panic if the people involved did not understand the relatively small degree of danger, and how to avoid it. If not understood, it could become a very effective psychological weapon.

Consequently, means for detecting and measuring radiation, and decontamination, are important. Equally important are understanding and training of the public.

b. High Explosive Bombs

High explosive bombs produce, on a lesser scale, the blast and fire damage involved in an atomic bombing. A study of bombing results in Europe indicates that a tremendous weight of bombs was required to destroy completely a factory building. Generally, damage was greater to wall bearing buildings than to buildings of steel or reinforced concrete frame construction. Such bombs were, in addition, responsible for destructive fires, particularly where the explosion caused leakage of gases, oils, and other inflammable material. When used in large number, the overall effect may be roughly comparable to that of an atomic bomb so far as fire and blast damage are concerned.

c. Incendiary Bombs

Incendiary bombs during the last war caused much greater fire damage than high explosive bombs. In an incendiary attack, fires start concurrently in buildings over a large area, and in a mass attack may produce "fire-storms" or "conflagrations."

The phenomenon of the "fire-storm," occurring in areas of high building density, in the absence of a strong ground wind, is caused by the self-generated inward draft of air at ground level to feed the fire. This inrush of air from all directions toward the fire center reaches high velocities. In such fire storms, temperatures of all combustible materials in the fire area are raised to the ignition point and a complete burn-out occurs. The fire-wind itself, however, confines the fire and thus limits its spread. Fire fighting cannot be effective within the storm area, but is effective on the perimeter of the storm.

The second type of mass fire is the "conflagration." In the presence of a strong ground wind, a potential fire storm will become a conflagration. The conflagration will wreak even greater havoc than the fire storm for an extended wall of fire will sweep before the wind until it has engulfed all combustible material within reach. On the windward and parallel sides of a conflagration, fire fighting can be effective.

d. Guided Missiles

Developments in the field of guided missiles make it necessary to consider this weapon one which an enemy may use in the event of war. The effect of such an attack would be similar to that of a conventional air attack, the nature and degree depending upon the type of warhead used and the number of missiles the enemy is capable of delivering.

2. CHEMICAL ATTACK

It is probable that the enemy has stocks of toxic gases and means of delivering them in effective quantities. Of greatest concern, are the nerve and blister gases which are persistent. Persistent gases are more likely to be used by the enemy in industrial areas because they are lethal and make the area untenable for some time.

3. BIOLOGICAL WARFARE

Biological warfare is the use of disease germs for purposes of war. The following facts are pertinent:

(a) A determined and resourceful enemy could employ the agents of biological warfare against us with possible devastating effect.

(b) Such agents might be disseminated by saboteurs before or after open war, or as part of an overt attack.

(c) Biological warfare could be directed against humans, animals, food and industrial crops.

(d) An enemy with a reasonably modern, scientific establishment can produce effective agents in adequate quantities.

(e) Agents capable of being used for biological warfare may be imported surreptitiously, or they may be produced within the United States by workers in clandestine laboratories.

Measures to be taken to minimize the effects of enemy attack are included under the Section on Active Measures Minimizing Effects of Enemy Attack. (Part VIII, Section E)

Part VIII

PROTECTIVE MEASURES

A. FACTORS INFLUENCING PROTECTIVE MEASURES

Protective measures include all actions, measures and techniques, employed to protect the personnel, products or service, premises, and processes, of the petroleum and gas industries from hazards inherent in the production or service operations, espionage, sabotage, and enemy attack. Accordingly, protective programs should be designed and implemented to reduce lost time and damage occasioned by ordinary operating hazards such as fire, accident, disease or illness and Acts of God, and to achieve security of information, prevention of sabotage, prevent reduction in productive or service capability, and to permit quick and efficient restoration of production or service after an emergency or disaster.

The scope and character of a protective program to be employed in any petroleum or gas system or facility should be no more extensive and no more limited than is warranted by an evaluation of the criteria set forth under *SELECTION OF VITAL FACILITIES,* (PART VI), and the following criteria.

1. The imminence of a hazard.
2. The probable or calculated risk.
3. Compromise of security versus efficiency.
4. Practical limitations imposed by the physical characteristics of the system or facility.
5. Availability of capital.
6. Evaluation of potential damage.
7. Evaluation of management, labor, employee, and public relations.
8. Measures necessary to direct and control the security program.
9. Practicability.
10. Alternate measures or techniques which will provide adequate security protection.
11. Evaluation and appraisal of security capabilities with the effective utilization of available resources.

Each system or facility must continually evaluate its position in the light of the foregoing factors and devise protective programs consistent therewith. When applying the technique of graded protection, it must not be forgotten that the criticality of a system or facility may vary from time to time as its products or service becomes more or less essential to the national defense emergency or its share of the total of the Nation's production becomes greater or lesser. Further, the importance of a system or facility does not necessarily depend upon whether or not the system or facility is producing an end product.

The general principles of protective measures apply to all security programs although the extent to which they apply varies widely according to such factors as:

1. Size, location and topography of property.
2. Type of system or facility.
3. Character of product or products or services.
4. Size of system or facility.
5. Character and importance of neighboring activities.
6. Availability of manpower for operations and security protection.
7. Availability of special materials and equipment for protection.
8. Time.
9. Cost.
10. Labor aspects.
11. Other managerial considerations.

Therefore, the following discussions of various security elements deal with them in principal rather than in minute detail. The protective program for a particular system or facility will have to be cut to meet the specific requirements of the system or facility.

Some facilities essential to the manufacture and delivery of vital products are especially important because they constitute limiting factors in an integrated series of operations. These "bottlenecks" occur in most every facility and are deserving of special consideration in the application of protective measures. These "bottlenecks" may be a crude, products, or gas pipe line, a refinery, a restricted waterway used by tank vessels, a natural gasoline plant, a strategic terminal, a supply of chemicals, or an auxiliary supply essential to the manufacture of vital petroleum products. All "bottleneck" facilities are not of equal importance because one may be capable of producing or handling many times as much vital material as another.

Other areas, such as the following, are deserving of special consideration in the application of protective measures.

Refineries, Compressor and Pump Stations

1. Communications.
2. Water Supply.
3. Power Supply.
4. Pumps, compressors and auxiliary equipment.
5. Docks and maritime facilities.
6. Electronic control equipment.
7. High pressure lines.
8. Valves in process control.
9. Facilities which are inherently vulnerable to sabotage.
10. Specialized equipment which is difficult to replace.
11. Components of supply which are susceptible to disruption or contamination.

Gas and Oil Fields

1. High pressure areas of substantial reserves.
2. High pressure areas producing special crudes of vital importance to the national defense emergency.
3. Individual gas wells capable of very large production.
4. Water, flooding and repressuring equipment, especially that in large recycling plants which are difficult to replace.
5. Producing property, damage to which may endanger important military, industrial and commercial operations.
6. Offshore producing operations.
7. Large central compressor and pumping stations and natural gasoline plants.
8. Individual wells. In a large majority of cases, the protection of individual wells may be impractical and unnecessary.

Pipe Lines

1. Pipe line pumping and compressor stations.
2. Water crossings and appurtenances.
3. Valves, gates, checks.
4. Power.
5. Regulation stations and control equipment.
6. Locations where important adjacent facilities may be damaged.

Compounding Plants

1. Process control equipment.
2. Mixing tanks.
3. Ingredients. Protected from contamination and spoilage.
4. Products. Protected from contamination and spoilage.

Products

1. Sources at which contaminants or additive spoilers may be introduced.
2. Products shipments for important facilities.
3. Products shipments which may be utilized as an initiator or destroyer of important facilities.
4. Unloading or transfer points and docks.

B. GENERAL SECURITY MEASURES

The general security measures outlined below are intended to serve the following purposes:

1. Provide a basis for planning and implementing protective programs.
2. Provide a basis for evaluating protective programs.
3. Achieve greater uniformity in protective programs.
4. Achieve greater consistency between protective programs.
5. Avoid excessive protective measures.
6. Provide more specific security guidance and assistance to management.

The application of the following general security measures will vary in degree by virtue of importance, scope, concentration, criticality and vulnerability to hazards inherent in the industry, espionage sabotage, probably air attack, damage, or theft. For similar reasons different areas within a facility may have varying degrees of security importance. To meet these situations and at the same time to facilitate operations and simplify the application of security measures, further segregation or compartmentation of individuals, activities, materials, and equipment may be required.

1. RESTRICTED AREAS

Segregation or compartmentation may be accomplished by establishing restricted areas. Restricted areas are established after such determinations as:

a. Critical areas, facilities, and portions of facilities have been made.

b. The individuals requiring access to these critical areas to perform their normal functions.

c. The type of information that should be protected.

d. The location of individuals requiring this type of information.

e. The degree which the establishment will unreasonably hinder or delay personnel or operations.

f. The possibility of regrouping of individuals and facilities or portion of facilities into one clearly defined area.

g. The possibility of using existing or parts of existing fences, barriers, protective alarms, protective lighting, etc., to provide adequate security.

h. The minimum expenditure of funds to establish an adequate restricted area.

i. The practicability.

The following basic security measures are required for all restricted areas:

(1) A clearly defined perimeter barrier.

(2) A personnel identification and control system.

(3) All points of access or egress guarded or under automatic alarm protection.

(4) Special consideration as to the desirability of protective lighting.

(5) Security and administrative arrangements for determining the need for access and the method of approval for access to the area.

(6) Escort procedures.

(7) Other security measures may be required depending on local circumstances.

The measures that follow have general application to the petroleum and gas industries as a whole.

2. ORGANIZATION

The protective organization for a petroleum or gas system or facility for security will depend almost entirely upon the size, criticality and vulnerability of the system or facility, the number of its personnel, and the added cost which may be assumed for this operation.

However, successful system or facility protection depends upon the interest and skill of those who devise and administer the program. It requires complete coordination between management and workers, and between the system or facility and the community and government. The normal and regular organization of the system or facility should be adapted to meet the requirements necessitated by the national defense emergency and should provide for the following functions:

(1) Analyzing the criticality and vulnerability of the system or facility and community to determine how great are the hazards and where the hazards are most likely to develop.

(2) Analyzing the existing protection system to determine the adequacy of the system in the light of hazards involved and to establish such additional protective measures as may be necessary.

(3) Training employees to observe protection regulations and to understand the reasons and purposes of the various regulations.

(4) Training key personnel in protection functions so that they may organize and direct workers under them in emergency.

(5) Establishing and maintaining cooperative procedures between management and workers to secure suggestions and information from workers, assign protective responsibilities, and aid in the harmonious and efficient operation of the program.

(6) Establishing coordinated working relationships with the entire community civil defense organization.

The proper discharge of the foregoing functions, as well as the vital importance of the matter to management and workers, requires that the responsibility for protection be placed in a position of top level authority so that safety and security problems will receive equal consideration with production, sales, and other management functions.

a. Security Director

The complexity of the problems of protection clearly points to the necessity for delegating to one individual the responsibility for protection operations. Whether the assignment of this individual is full or part time depends upon the size and nature of the system or facility. A suggested title for this individual is "Security Director." The duties of the Security Director will be:

(1) To analyze the need for and to devise protection measures.

(2) To administer and supervise the operation of the protection measures.

(3) To organize and train employee service groups.

(4) To educate employees in protection and to develop employee cooperation and assistance in all phases of the protection program.

(5) To maintain liaison with local civilian defense agencies and to integrate the system or facility and its programs and organizations into the community civil defense plant.

(6) To maintain relations with other system or facility security directors to enable mutual assistance in the solution of problems, and the sharing in emergency, of supplies, equipment, productive capacity, and personnel.

(7) To direct, plan, organize and coordinate all system or facility civil defense aspects in the event of attack, including fire-fighting, damage, control, rescue, evacuation, medical service, and restoration of the system or facility.

Emergency and disaster programs should be based by the Security Director, to the extent feasible, upon existing programs maintained as part of the normal business practices of the system or facility involved.

An emergency or disaster function for which no counterpart is found in existing system or facility programs must be developed to afford the necessary emergency or disaster services for the protection of employees and property during and after direct attack. In the establishment of the emergency or disaster protection program, full use should be made of the existing service departments, such as

fire, medical, repair, and guard organizations. The departments should continue to function as usual, coordinated and guided by the Security Director, except in emergency or disaster, at which time they should operate as a unit of the emergency and disaster program under the full administration of the Security Director. The personnel of these units should be augmented as necessary, and trained to cope with all types of emergencies and disasters.

3. PERSONNEL

Employees are in a very favorable position for the accomplishment of espionage and sabotage. Since applicants may become employees and since employees are in this favorable position, care should be exercised in the screening, investigation and clearance of personnel.

There are four general categories of potentially undesirable applicants or employees in addition to the known subversive, namely:

(1) One susceptible to recruitment by subversive elements.

(2) Habitually dissatisfied or disgruntled employees.

(3) Individuals exhibiting habitual criminal tendencies.

(4) Accident prone or careless individuals whose acts or failure to act may have the same results as an act of sabotage.

(5) Absentees.

These categories have been stated merely to point out the investigative and clearance problem. Criteria to be applied to eliminate undesirables are discussed under the section on PERSONNEL LOYALTY DETERMINATIONS, PART VIII, Section B 3 b.

The most difficult category to determine is that group susceptible to recruitment by subversive elements.

Subversive elements generally recruit espionage and sabotage agents by applying general principles to determine the agent's suitability such as:

(1) Ability to withstand an investigation.

a. Clear background.

b. A background that can be covered or documented to withstand an investigation.

c. A present employee who may not be subject to an extensive investigation.

d. An individual who is expert in a particular field with a creditable explanation of any unfavorable information revealed by an investigation.

(2) Free access to the vital information or the facility to be sabotaged.

a. Employee.

b. Applicant who would become an employee.

c. Non-employee having access.

(3) Susceptible to recruitment by one or more of the following means:

a. Ideological appeal.

b. Play on the emotions. .

c. Promise of money or a material reward.

d. Promise of prestige or power.

e. Appealing to the spirit of adventure.

(4) No objectional personal characteristics that would invite attention, such as:

a. Openly expressing sympathy with subversive ideologies.

b. Inability to keep a secret.

c. A criminal record of heinous or felonious crimes.

d. Instability.

e. Habitual drinking or drug addiction.

f. Known association with communists or communist dominated or sponsored organizations.

(5) Possibility of exercising complete control over the individual after recruitment.

(6) Possessed of special skills or training.

Subversive elements do not always rigidly observe the above standards and have been known to violate most of them from time to time.

However, the proper application of personnel security measures will reduce the calculated risk. Personnel investigations serve as a deterrent and a screening process to uncover unfavorable information on applicants and employees.

While management is primarily responsible for the safety of its property, labor has an even more vital and personal interest in protecting itself from injury, loss of life, or loss of livelihood through the activities of subversives. *A successful protection program must have the cooperation of organized labor and employees.*

a. *Security Education, Information and Training*

Each loyal employee is a personally interested assistant in the successful operation of protection programs. The value of this great reservoir of assistants is incalculable, for as a group, they—

(1) Know all details of operation more completely than either management or undercover men;

(2) Know their fellow workers far more intimately; and

(3) Can be shown the need of exercising an ever-present and all inclusive surveillance.

Thoroughly effective cooperation of employees cannot be expected or secured without education and training in the problems involved and the

discipline required. The more important points involved in which employees should be educated are—

(1) Willing acceptance of the unpleasant fact that all employees must be inconvenienced by the many rules and regulations designed to trap or thwart the few subversives.

(2) The dangers of talking business away from the job.

(3) The dangers of hysteria and disaffection which may be inspired by subversive organizations.

(4) The dangers of spreading unconfirmed rumors.

(5) The detection and reporting of trespassers.

(6) Observance of suspicious characters and their actions.

(7) Avoidance of unwarranted approaches by strangers anywhere.

(8) Avoidance of association with dubious characters.

(9) Avoidance of suspicious promotional offers involving lurid business or financial opportunities.

(10) Noting and reporting unusual equipment failures and accidents.

(11) Familiarity with the tactics of spies and saboteurs.

To be effective, educational work of this character must be continuous. Furthermore, it must be sufficiently appealing to capture the interest and imagination of the employee. Experience indicates that the most effective form of education is the informal, on-the-job instruction conducted by the employee's immediate supervisor. Here it is possible to use actual, everyday examples to illustrate general principles, thus fixing the problems and responsibilities more firmly in mind than by depending entirely upon classroom or textbook instruction. A written text usually serves better as reference material for the instructing supervisor than for the employees whom he instructs.

b. *Personnel Loyalty Determinations*

Assurance of loyalty is important in peacetime but it is extremely important in time of a national defense emergency. Accordingly, self-sufficient procedures for loyalty determination must be incorporated by the system or facility in its standard personnel policies. Some help may be secured in personnel investigations and clearance from Government Agencies when the system or facility is engaged in classified contracts.

Investigation of actual or suspected espionage or sabotage is a function of the Federal Bureau of Investigation. If an employment investigation indicates a basis for suspicion of espionage or sabotage activities, this information should be reported to the nearest field office of the Federal Bureau of Investigation. (Also, see PART VIII, Section B 6)

It must not be assumed that the Federal Bureau of Investigation will, either directly or indirectly, inform management or the security director of subversives or suspected subversives employed in the system or facility.

Investigations should be limited to personnel having access to vital information or restricted areas involving critical operations. The techniques for limiting the number of personnel requiring investigation and clearance have been discussed previously.

Fingerprinting is necessary to assure positive identification, the most important requisite to investigation of personnel. Although the Federal Government is not accepting fingerprint records from private industry for processing purposes, some assistance may be obtained from other law enforcement agencies and private investigators and it is recommended that duplicate sets of prints be obtained. Fingerprint Cards (11) *, U. S. Government Form No. 16-63416-1 may be obtained for this purpose from the U. S. Government Printing Office, Washington 23, D. C., at a price of $1.50 per hundred. In this connection, it is most important that fingerprint impressions be properly and legibly made. A pamphlet entitled "How to Take Finger Prints" (58) * can be obtained at no charge by addressing requests to the Identification Division, Federal Bureau of Investigation, Department of Justice, Washington 25, D. C. This pamphlet is illustrated and also contains suggested methods for the fabrication and procurement of necessary equipment.

It is exceedingly important that complete answers are supplied in executed questionnaires and that full signatures be obtained.

(1) APPLICANTS

Adequate application forms should be completed by every applicant before consideration for employment. The information included in the personnel security questionnaire should be of sufficient detail to facilitate an investigation. A suggested personnel security questionnaire has been included in Appendix "B".

The personnel security questionnaire should be screened for completeness, undesirables eliminated and a determination should be made as to the necessity for investigation based on access to vital information or restricted areas.

A responsible management official should then conduct sufficient investigation to assure that the applicant's character, associations, and suitability for employment are satisfactory.

* See Bibliography

The following sources may be helpful in securing employment investigative data:

(1) State and local police.

(2) Former employers.

(3) References other then those furnished by applicant.

(4) Public records.

(5) Credit agencies.

(6) College or University professors.

Due consideration should be given to the advisability of securing statements of individuals of former employers as to previous investigations and clearances by responsible Government Agencies. This consideration will be limited by the following:

(1) The type of investigation performed.

(2) The period covered.

(3) The date of the investigation.

(4) The Government Agency responsible for investigation.

(5) The Government Agency making clearance determination.

(6) Receipt of verification of clearance from responsible Government Agency.

(7) The type of investigation performed meets the standards adopted by management.

(8) The elapsed time of the last investigation and clearance is two years or less.

(9) This procedure does not violate an existing law, executive order or Federal administrative regulations.

In requesting investigative data from any of the above sources, it is suggested that the following minimum information be furnished, as appropriate, to properly identify the applicant and minimize erors in identity.

(1) Full name and other names or aliases used.

(2) Personal description.

(3) Date and place of birth.

(4) Present and immediate previous address with dates.

(5) Employment present and last.

(6) Social Security number.

The above information on a short Personnel Security Questionnaire is all that may be required for contractor employees in performing an investigation.

Consideration should be given to accomplishing personnel investigations by contract arrangements with reputable private investigative organizations.

In either event the period covered by a background investigation should be the latest 10 years. However, if unfavorable information is disclosed the period may be greater in order that the unfavorable information may be verified or developed further.

In the event that the applicant was in the Military Service and presents an honorable discharge, the period covered by the investigation may exclude the period of military service.

A management official should be responsible for reviewing the results of investigations for such things as:

(1) Unfavorable information.

(2) The need for further investigation to further develop information reported.

(3) Completeness as to investigative coverage.

(4) Discrepancies between the information included in the personnel security questionnaire and the investigative report.

(5) Insuring that there are sufficient reasons or details to support or provide for proper analysis of information reported. For example: Mr. X states that he believes the applicant is a communist. The individual performing the investigation should determine and provide such additional information on Mr. X as:

(a) What is Mr. X's definition of a communist?

(b) What is Mr. X's education and experience?

(c) What has been the extent of contact with the applicant?

(d) Has Mr. X had any recent quarrels with the applicant?

(e) Did Mr. X know of anybody else who believes that the applicant was a communist?

(f) What particular acts or statements of the applicant influenced Mr. X in making this statement.

(g) Mr. X's general reputation in the community.

(6) Has the investigating agent or informant been biased in reporting investigative data?

(7) Are statements contained in the investigative report subject to more than one interpretation?

(8) Is the investigation adequate after considering all of the above?

When investigative reports are adequate, a responsible management official must make a security clearance determination in a manner consistent with traditional American concepts of justice and rights of citizenship. The decision as to security clearance is an over-all, common-sense judgment made after consideration of all the relevant information as to whether or not there is risk that the granting of security clearance would endanger the common defense or security. If it is determined that the common defense or security will not be endangered, the security clearance should be granted.

To assist in making these determinations, management must adopt criteria in regard to the applicant and his spouse which will establish a reasonable

assumption of a security risk, such as whether the applicant or his spouse has:

1. Committed or attempted to commit, or aided or abetted another who committed or attempted to commit, any act of sabotage, espionage, treason, or sedition.

2. Establish an association with espionage agents of a foreign nation; with individuals reliably reported as suspected of espionage; with representatives of foreign nations whose interests may be inimical to the interests of the United States. (Ordinarily this would not include chance or casual meetings; nor contacts limited to normal business or official relations.)

3. Held membership in or joined any organization which has been declared by the Attorney General to be Totalitarian, Fascist, Communist, subversive, or as having adopted a policy of advocating or approving the commission of acts of force or violence to deny others their rights under the Constitution of the United States, or as seeking to alter the form of government of the United States by unconstitutional means, provided the individual did not withdraw from such membership when the organization was so identified, or otherwise establish his rejection of its subversive aims; or, prior to the declaration of the Attorney General, participated in the activities of such organization in a capacity where he should reasonably have had knowledge as to the subversive aims or purposes of the organization.

4. Publicly or privately advocated revolution by force or violence to alter the constitutional form of Government of the United States.

5. Deliberately omitted significant information from or falsified a Personnel Security Questionnaire. In many cases, it may be fair to conclude that such omission or falsification was deliberate if the information omitted or misrepresented is unfavorable to the individual.

6. Violated or disregarded security regulations to a degree which would endanger the common defense or security.

7. Been adjudged insane, been legally committed to an insane asylum, or treated for serious mental or neurological disorder, without evidence of cure.

8. Been convicted of felonies indicating habitual criminal tendencies.

9. Been, or is, addicted to the use of alcohol or drugs habitually and to excess, without adequate evidence of rehabilitation.

10. Sympathetic interest in totalitarian, fascist, communist or other subversive political ideologies.

11. A sympathetic association established with members of the Communist Party; or with leading members of any organization set forth in paragraph 3, above. (Ordinarily this will not include chance or casual meetings, nor contacts limited to normal business or official relations.)

12. Identification with an organization established as a front for otherwise subversive groups or interests when the personal views of the individual are sympathetic to or coincide with subversive "lines." See list in Appendix B.

13. Identification with an organization known to be infiltrated with members of subversive groups when there is also information as to other activities of the individual which establishes the probability that he may be a part of or sympathetic to the infiltrating element, or when he has personal views which are sympathetic to or coincide with subversive "lines."

14. Residence of the individual's spouse, parent(s), brother(s), sister(s), or off-spring in a nation whose interests may be inimical to the interests of the United States, or in satellites or occupied areas thereof, when the personal views or activities of the individual subject of investigation are sympathetic to or coincide with subversive "lines" (to be evaluated in the light of the risk that pressure applied through such close relatives could force the individual to reveal sensitive information or perform an act of sabotage).

15. Close continuing association with individuals, (friends, relatives, or other associates), who have subversive interests and associations as defined in any of the foregoing types of derogatory information. A close continuing association may be deemed to exist if:

a. Subject lives at the same premises with such individual;

b. Subject visits such individual frequently;

c. Subject communicates frequently with such individual by any means.

16. Association where the individuals have enjoyed a very close, continuing association such as is described above for some period of time, and then have been separated by distance; provided the circumstances indicate that a renewal of contact is probable.

17. Conscientious objection to service in the Armed Forces during time of war, when such objections cannot be clearly shown to be due to religious convictions.

18. Manifest tendencies demonstrating unreliability or inability to keep important matters confidential; wilful or gross carelessness in revealing or disclosing to any unauthorized person vital information; abuse of trust, dishonesty; or homosexuality.

The above criteria are not all inclusive and are set down merely to indicate how criteria for determining security clearance may be established and applied.

(2) EMPLOYEES

All employees having access to vital information and restricted areas should be investigated and cleared.

The same procedures as those outlined for applicants should be followed.

Employees are in a different position than applicants as to denial of clearance. Management simply may not hire an applicant who is considered a security risk, while management may do one of three things when an employee is considered a security risk.

1. Discharge the employee for any number of administrative reasons.

2. Transfer the employee to a position where he will not have access to vital information or restricted areas.

3. Secure a position for the employee in another industry or commercial enterprise which is not vital to the national defense.

When there is doubt as to a security risk, the doubt should be resolved in favor of security.

The cooperation of organized labor and employees is a prerequisite to any successful program for the suspension or containment of undesirables. This cooperation may be obtained by the formation of Labor-Management Committees. These committees should review the information on undesirables and recommend clearance or denial of clearance. Management is then responsible for taking appropriate action.

Information furnished these committees should not identify the informant, especially if such source has requested that the information be kept in confidence. All security information and investigative reports should be carefully safeguarded.

(3) NON-EMPLOYEES

The investigation of non-employees desiring access to a restricted area may not be required if such personnel are duly authorized and are accompanied by a responsible escort. Special cooperation should be given to special agents of the Federal Bureau of Investigation desiring access to restricted areas for official business.

Non-employees should include such individuals as:

1. Union officials.
2. Contractors' personnel.
3. Sub-Contractors' personnel.
4. Outside maintenance personnel.
5. Vendors.
6. Business visitors.
7. Manufacturers' representatives.
8. Delivery personnel.
9. Consultants.

Access of non-employees to restricted areas is to be discouraged except those with legitimate business reasons.

c. *Aliens*

Careful judgment should be exercised by management in the employment of aliens, because of the increased possibility of introducing subversive elements into the system or facility. An alien holding first citizenship papers is still an alien within the intent of the law.

A list of all aliens employed by the system or facility should be maintained with a record of their alien registration number. Data should be available indicating the type of work on which individual aliens are employed and whether or not they have applied for, or received, first citizenship papers.

Regulations which prohibit the employment of aliens on certain Government contracts provide in essence that no alien may be employed on classified contracts without written permission of the Government Agency having jurisdiction.

4. ACCESS CONTROL

When it becomes necessary to establish restricted areas, a system controlling access to them is required.

The control system employed should:

1. Provide a means of identifying personnel who are authorized to have access.

2. Facilitate control of the admission of personnel.

3. Facilitate control of the egress of personnel.

4. Provide a visible means of easily recognizing any limitations or access within restricted areas.

The arrangements governing the identification and control of access of personnel to an area should, of course, be related to the relative security importance of the area and to the category of persons involved (employees-visitors).

Identification and control arrangements should not only be effective in preventing unauthorized entry and access but should also take into consideration the efficiency of facility operations. They should be workable, understandable, and as simple as possible and at the same time effective.

a. *Pass and Badge System*

Small areas employing not over 30 persons per shift who are personally acquainted and have a low rate of turnover may be controlled by personal recognition. Where the area is large or where the number of employees exceeds that which can easily be personally recognized by the guard or the area supervisor, a personal identification system is essential. The most practicable means of

identification at large facilities is by an authorized pass or badge.

Where a pass or badge is used, it should be of "tamperproof" construction. (In general, metal-rimmed or plastic-envelope devices are not considered as being tamperproof.) Laminated or embossed passes and badges are considered to meet this requirement when they incorporate the following features:

1. A distinctive and intricate background design, which is difficult to reproduce by normal photocopying.

2. A clear photograph, at least 1 inch in its smallest dimension, and legible serial number. Where both passes and badges are employed, the photographs should be made from the same negative. Individuals should be rephotographed when necessary to reflect any significant physical changes in facial appearance but in no event less often than every 5 years.

3. Inks or dies on some part of the face of the device which are noticeably affected by such heat or erasure as would be necessary to relaminate or alter the device.

4. Additional information on the pass to identify the person to whom it is issued, usually including name, signature and thumbprint.

5. Where applicable, code denoting area for which a badge is valid.

6. Signature (or facsimile) of validating official.

7. Serially numbered.

8. Sturdy in construction.

9. Resistant to fumes inherent in the industry.

10. Some secret characteristic known only to management.

It is recognized that practically any badge or pass can be altered or reproduced by determined individuals sufficiently skilled in printing, engraving, and photography. However, badges and passes made in accordance with the above are sufficiently difficult to alter or reproduce to be acceptable as a deterrent. Additional protection against forged credentials may be afforded by exchange systems and by the rigid control and accountability exercised over the valid media. At locations where credentials which are extremely difficult to duplicate or alter are considered necessary, the following commercially available materials may be used.

1. Watermarked insert paper prepared with a distinctive watermark specifically for the location. The difficulty and expense of duplicating watermarks makes this an effective security feature.

2. Readily visible cross-threads or wires within the plastic cover sheets of the badge or pass which will make obvious any alteration of the device such as superimposing a photograph, signature, number, etc., over the original and then relaminating with a third piece of plastic.

3. Sensitized plastic material on which the photograph is printed, made to the same chemical formula as the transparent plastic covers. When this is used, the photograph panel of the paper insert is cut out so that, in laminating, the front and back transparent plastic sheets and the plastic photograph flow together forming a solid piece of plastic material.

4. A paper for use as insert material which loses its fibrous strength while being heated during the laminating process. Any attempt to separate this paper or to peel off the plastic from it will result in a physical disintegration of the weakened, brittle paper.

5. Ink of a type which bleeds and/or changes color when exposed to chemical solvents which dissolve the plastic covers.

6. Fluorescent inks which may or may not be normally visible, but which are visible under ultraviolet light.

7. An embossed plastic or intricate design and/or such other similar materials as will accomplish the desired purpose of preventing or making counterfeiting difficult.

b. *Employee Identification and Control System*

The arrangements for the identification and control of employees at a facility should include the following:

(1) Designation of the various restricted areas involved.

(2) Description of the various identification media involved and the authorization and limitations placed upon the wearer.

(3) Mechanics of identification at times of entering and leaving each restricted area, as applied to both employees and visitors, including off-shift hours.

(4) Details of where, when, and how badges shall be worn.

(5) Procedures to be followed in case of loss or damage to identification media.

(6) Procedures which will recover employee badges on termination of employment.

(7) A procedure to reissue new identification media when 1 percent have been lost, or unaccounted for.

c. *Visitor Identification and Control System*

For the purpose of this Guide, the term "visitors," in addition to its normal connotation, is defined as including employees and others who require infrequent access to a restricted area, or to whom permanent employee-type identification for such area has not been issued.

The primary responsibility for the control of visitors to and within restricted areas rests with the official directly responsible for the facility.

Arrangements for the identification and control of visitors should include the following:

(1) Positive method of establishing the authority for admission of visitors, as well as any limitations relative to access.

(2) Positive identification of visitors at the facility or restricted area (to be visited) by means of personal recognition, visitor permit, or other identifying credentials. Employee to be visited should be contacted to ascertain validity of visit.

(3) Availability and use of visitor registration forms and records which will provide a record of identity of visitor, time and duration of visit, and other pertinent control data.

(4) Availability and use of visitor passes. Such passes should be numbered serially and indicate the following:

(a) Bearer's name.
(b) Area or areas to which access is authorized.
(c) Escort requirements, if any.
(d) Time limit for which issued.
(e) Signature (or facsimile) and title of validating official.

(5) Availability and use of visitor badges embodying applicable features similar to those established for employee badges; and, in addition, distinctive characteristics which will make obvious that the wearer is a visitor; escort requirements, if any, and any limitations as to access.

(6) Procedures which will insure supporting personal identification in addition to a check of visitor badges or passes at restricted area entrances.

(7) Procedures for escorting visitors having limitations relative to access through areas where an uncontrolled visitor, even though conspicuously identified, could acquire information for which he is not authorized.

(8) Controls which will recover visitor passes or badges on expiration, or when no longer required.

(9) Twenty-four-hour advance approval when possible.

d. *Application*

To be effective, it is essential in an impersonal identification system that guards at control points carefully compare each badge to its wearer and, where a badge-exchange arrangement is utilized, that guards make a three-way comparison of the badge, the pass, and the individual. Close administrative supervision and follow-up of personnel charged with checking identification media are necessary to keep an identification system from becoming careless and ineffective.

Make-up and issue of identification media should be carefully controlled to minimize the possibility of counterfeiting or theft, to insure return and destruction upon termination of employment, and to promptly invalidate lost, mutilated, or defective badges. Badges should be recorded and controlled by rigid accountability procedures. As an operating practice, a lost badge should be replaced by a new one of different number or otherwise not identical to the one lost so that the lost badge may be effectively invalidated.

Badges should be of such design and appearance as will permit the facility guards and employees to recognize the authorizations and limitations applicable to the wearers quickly and positively.

Contractors' employees performing work in a restricted area should be provided with and be required to wear a distinctive badge. There are three general types of contractors' employees.

1. Employees on substantial service or construction projects requiring a considerable period of time to complete. The contract work area should be isolated by means of a fence or other effective barriers. When possible, contractors' employees should enter the work area directly without entering the restricted area. Where it is necessary for the contractors' employees to enter a restricted area to reach the work area, the guard force personnel should insure that contractors' personnel go directly to the work area without loitering or straying within the restricted area.

If the work area is segregated and abutting restricted areas or portions of abutting restricted areas are properly guarded, contractors' employees do not have to be investigated and cleared by management. Contractors' employees should wear distinctive badges and their loyalty should be vouched for by their employer.

2. Employees performing work at regular or irregular intervals and for a short working period within a restricted area should be handled by the same procedure adopted for the control of visitors.

3. Employees performing continuous service for the facility within a restricted area should be handled by the same procedures adopted for regular facility personnel.

Enforcement of access control systems for restriced areas rests primarily on the facility guards. But it is essential that they have the full cooperation of the employees, who should be educated and encouraged to assume this security responsibility. Employees should be instructed to consider each unidentified or improperly identified individual as a trespasser. In restricted areas where passes are limited to particular zones, employees should report movements of individuals to unauthorized zones.

5. SAFEGUARDING CLASSIFIED SECURITY MATTER

Classified security matter is information, data, documents, material, products, etc., which must be safeguarded in the interest of national security. Security matter should not be confused with matter such as personnel records, high level company decisions, unpatented processes, etc., which are given a confidential classification by management for purely administrative reasons.

The term, safeguarding, includes care in production, transmission, handling, disseminating and storage, and stages of an operation to assure that unauthorized individuals do not have access to classified security matter.

A responsible government agency assigns the appropriate (appears earlier, e.g. P. 22) security classification. Federal Statutes, Executive Orders, etc., govern the procedures for safeguarding classified security matters. These procedures are basically the same as have been in effect in the various branches of the Federal Government for many years.

Security classifications commonly in use are "Top Secret," "Secret," "Confidential," or "Restricted," depending on the degree of importance to the national security. "Top Secret" covers matter of utmost importance. "Restricted" requires the minimum of precaution. There is one other highly important classification, "RESTRICTED DATA," which pertains to atomic energy matters and should not be confused with the minimum security classification, "RESTRICTED." This "RESTRICTED DATA" classification would not normally be of concern to the petroleum and gas industries unless they had a contractual relationship with a governmental agency involving atomic energy matters.

a. *Administrative Precautions*

The procedure for handling and controlling classified security matter is designed primarily for Federal Agencies and other organizations having a classified contract with Federal Agencies. In such cases, the Federal Agency involved assures that the recipient is authorized to receive, requires such classified matter to discharge the classified contract obligations, and is familiar with the current regulations for the protection of classified security matter.

In cases of frequent contact, a Federal Agency will often merely add a warning statement on classified security matter. This warns the recipient that the matter contained therein is important to the national defense and its disclosure to unauthorized persons is prohibited by law.

Management is responsible for the protection of classified security information which may come into its possession. Security regulations furnished by the Federal Agencies releasing such information to management must be complied with in full. Active vigilance on the part of management, coupled with alert anticipation of the avenues by which the information may be obtained under the circumstances prevailing in the particular system or facility must be employed to supplement the standard procedures prescribed in such Federal regulations. Particular attention should be paid to employees handling such information, their loyalty, discretion, character, and susceptibility to bribery, flattery or recruitment. Some of the administrative precautions which should be employed are as follows:

(1) Persons handling classified security or vital information should be separated from other employees and should work in restricted areas where absolute security can be maintained.

(2) When not in use, classified security or vital information should be preserved in locked combination safes. Safe combinations and keys to restricted areas should be issued only to a limited number of trusted employees. Safe combinations should be changed frequently and should be changed immediately whenever any person knowing the combination leaves the employment.

(3) Control of the number of copies of correspondence, plans or other documents containing classified security information must be exercised to assure that extra copies are not made and delivered to agents outside the system or facility.

(4) Waste and carbon paper from administrative offices, engineering departments, drafting rooms and blue-print rooms and other departments using classified security or vital information must be disposed of by burning or shredding so that no classified material can be salvaged and used. Janitors and charwomen, due to their access to all parts of a facility, have unusual opportunities to obtain classified security or vital information and by reason of low salaries may have more than ordinary inducement to do so. Such persons should, therefore, be kept under reasonable surveillance.

Unclassified vital information originating within the system or facility may be of as great importance to the espionage agent as information released to the system or facility by governmental departments. Unless the origination of such vital information is directly under the supervision of a governmental department it may not be given a formal security classification. Such information, however, should be protected with the same zeal and by the same procedures accorded classified security information. Management, in the exercise of sound discretion, must assume responsibility for its own classification of such vital material and its protection against espionage.

References:

Industrial Security Manual for Safeguarding Classified Matter, Department of Defense, Munitions Board, 13 December, 1951.*

Executive Order 10290, 24 September 1951, "Prescribing Regulations Establishing Minimum Standards for the Classification, Transmission, and Handling, by Departments and Agencies of the Executive Branch, of Official Information which Requires Safeguarding in the Interest of the Security of the United States.

b. *Protection and Duplication of Records*

Considerations must be given to safeguarding vital records such as: maps, plans, contracts, specifications, drawings, and other important data which are irreplaceable or require a long time to replace.

It may be advantageous to store duplicate copies at alternate remote locations to minimize the loss of the originals. In other cases, vital data should be copied on microfilm and dispersed to safe storage depositories in remote secured areas. Alternate custodians with right of access to these depositories should be designated from personnel who are employed in the vicinity.

If microfilming is employed, provision should be made for viewers and for equipment to reproduce data to working size copy.

6. SECURITY LIAISON WITH FEDERAL, NATIONAL, STATE, LOCAL AND PRIVATE ORGANIZATIONS

The petroleum and gas industries should establish a working relationship with the activities of those Federal, National, State, Local and private associations and organizations concerned with Security.

Emergency and disaster plans should be coordinated with State and Local Civil Defense Agencies and military authorities so that there will be complete understanding concerning relative spheres of activity during an emergency or disaster, thereby avoiding duplication of effort. Particular attention should be given to permit the movement of essential personnel and equipment during emergencies.

Details regarding warning of an air attack should be worked out with the local Civil Defense Headquarters.

Fire services should be arranged for with the local fire department. Medical and welfare services should be established through the County Coordinator of the State Civil Defense Commission.

Post raid activities should be adapted to local and state programs.

Security liaison with local authorities is desirable to insure that adequate consideration is given to the protection of vital facilities outside the perimeter of the system or facility but which serve the system or facility transportation, water, power, etc.

Security liaison with local and State police is important for coordinated effort in securing adequate protection to meet special conditions.

Assistance in training, planning, etc., may be obtained through liaison with State and local organizations such as police, fire, health, engineering services, etc.

The cooperation of State and local police should be sought in personnel investigations and the development of public record information.

Assistance in fire prevention and fire-fighting measures may be obtained through liaison with the National Board of Fire Underwriters or the National Fire Protection Association.

Assistance in safety and accident prevention programs may be obtained through liaison with the Oil and Gas Division, Department of the Interior; the Department of Labor; and the National Safety Council.

Assistance may be obtained through liaison with National Trade Organizations, representing segments of the petroleum and gas industries, in:

1. Drafting emergency restoration and rehabilitation plans.
2. Obtaining information on alternate sources of supply.
3. Fire, safety and other protective measures.
4. Maintaining an availability list of vital equipment that would be needed to restore a damaged facility to active production or service.
5. Maintaining an availability list of specialized personnel as a means of expediting reactivation of a system or facility.
6. Maintaining the necessary contact with appropriate governmental agencies to insure that the member petroleum and gas organization needs are made known.
7. Advising members on new legislation, protective measures, assistance, etc., that may help in developing protective programs.

The Federal Government is in a position to have the greatest knowledge of the over-all situation with regard to war plans needs and material output; the local government is in the best position to determine its needs for emergency facilities, location of spare facilities, local manpower, etc.; the system or facility operator knows intimately his facilities and operations. Each unit of government and industry must, therefore, know and be concerned with the protective functions, available

* See Bibliography

assistance and rehabilitation requirements necessary to provide continuity of production or service.

Suspicious action or subversive information should be reported promptly to the nearest field office of the Federal Bureau of Investigation. Particular attention is called to the jurisdiction of the Federal Bureau of Investigation in espionage, sabotage and related matters. Presidential directive gives the Federal Bureau of Investigation the responsibility of taking charge of investigative work in the above mentioned fields and request all enforcement officers and individuals to report all information bearing on the above to the nearest field representative of the Federal Bureau of Investigation. The nearest FBI office is listed on Page 1 of most telephone directories.

7. EMPLOYEE AND PUBLIC RELATIONS

The formulation, activation and application of protective measures for any petroleum or gas system or facility is the responsibility of the employees as well as of management. Operating personnel are in an excellent position to plan and implement those measures essential for security.

There should be a clear line of responsibility in each petroleum and gas system or facility from the chief executive to the manager or supervisor in charge of each property which is to have defense protection of its facilities. Each manager or supervisor should be given appropriate authority to adopt such protective measures as may be necessary to discharge his responsibility, especially in event of an emergency.

The full and active cooperation of employees and labor must be obtained to assure an adequate protective program. Management-employee committees and labor-management committees have been helpful in the formulation, activation and application of protective measures. The following areas are cited as examples of this:

1. Personal and process safety.
2. Metal Inspection.
3. Fire Prevention, Control and Extinguishment.
4. Employment Qualifications.
5. Adopting criteria to deter undesirables.
6. Elimination of undesirables.
7. Employee security education.
8. Personnel records and investigation of personnel.
9. Handling violations of protective measures.
10. Designating restricted area limits.
11. Reporting of suspicious acts.
12. Recruitment of applicants.
13. Psychological aspects, such as false rumors, attempts to create unrest, etc.
14. Strikes, slow-downs, etc.
15. Employee hearings and due process.

Another important element in formulating, activating, applying and maintaining a protective program is keeping the general public and employees adequately informed so as to bring about thorough understanding and support.

The use of communication media should be fully exploited to keep the public informed as to the industry's role in national defense and to recommend actions that private industry and the general public who depend on petroleum and gas products or services should take to implement the protective program or should take in the event an emergency or disaster occurs to the petroleum or gas system or facility.

The cooperation of owners of property traversed by pipe lines should be solicited, where this is considered feasible, to keep pipe line operators advised of any unusual occurrence which the property owners may observe.

Management of service organizations should be informed of appropriate security measures and what will be required of management of service organizations before admittance of their employees to restricted areas will be permitted. Examples of this are railroads, trucking companies, utilities, etc.

Employees and employee groups should be informed that protective measures are established for their protection and safety and to safeguard their livelihood.

8. INSPECTIONS AND REPORTS

a. *Managerial*

Management should perform frequent inspections and receive reports to assure itself of the sufficiency of the security programs. This procedure will be of assistance in maintaining the efficiency and continuity of the security program and providing revisions as required by changing conditions, as well as creating and maintaining interest.

b. *Others*

When it is necessary for authorized governmental agencies to make a security inspection, they should first arrange with top management to review the over-all program and decide on such facilities as should be inspected. The inspector should be accompanied by a representative of top management.

Any reports prepared by the inspector should be in cooperation with management, which should be furnished with a copy.

c. *Inspection Forms*

The instructions for completing the inspection report form for a system and a facility are included in this set of principles as Appendix B.

The inspection report form for a system is included in this set of principles as Appendix C.

The inspection report form for a facility is included in this set of principles as Appendix D.

The inspection report check list, which is utilized to determine the adequacy of the protective program, is included in Appendix F.

C. INDUSTRIAL SECURITY MEASURES

In analyzing the need for and the type and extent of the industrial security measures required at a facility, the following factors, among others, should be considered in planning an industrial security program.

(1) The classification of information, data, activities and/or strategic value of matter located therein.

(2) The importance of the facility to the continuity of essential production or service operations. (In evaluating this factor, the availability of alternate facilities which could be utilized in an emergency, and/or the availability of stockpiles of materials produced by the facility under consideration should be analyzed.)

(3) The vulnerability of vital equipment or materials to damage or theft.

(4) The location, size, and arrangement of the facility; and numbers of personnel involved.

(5) The need for integrating adequate security measures with operating requirements, and other local considerations.

(6) The probable duration of operations.

(7) The possibility or probability of expansion, retrenchment, or other changes in operations.

(8) The cost of alternate methods of providing adequate protection.

(9) After analysis and evaluation of these and other pertinent considerations, a physical security program should be designed in accordance with measures hereinafter set forth.

1. GUARD SERVICE

In accordance with established plans and procedures at the facility or facilities to which they are assigned and within the scope of their authority, guard forces achieve their purpose by a combination of actions, consisting principally of the following:

(1) Implement and enforce the system of personnel identification and control.

(2) Observe and patrol designated perimeters, areas, structures and activities of security interest.

(3) Apprehend persons or vehicles gaining unauthorized access to security areas.

(4) Check designated depositories, rooms, or buildings of security interest during other than normal working hours to determine that they are properly locked or are otherwise in order.

(5) Report to supervision, as a matter of prescribed routine under normal conditions, and as necessary in the event of unusual circumstances.

(6) Perform essential escort duties.

(7) Implement and enforce the established system of control over the removal of documents or material of security interest from security areas.

(8) Respond to protective alarm signals or other indications of suspicious activity.

(9) Act as necessary in the event of situations affecting the security of the facility including fire, industrial accidents, internal disorders, and attempts to commit espionage, sabotage, or other criminal acts.

(10) Otherwise generally safeguard data, materials, or equipment against unauthorized access, loss, theft, or damage.

In determining the need for a guard force in the security program for a facility, all factors bearing on the security interest at such facility must be considered, as well as conditions relating to the nature, location, and layout of the facility and the incorporation and effectiveness of other elements in such program. As these factors may differ widely in individual cases, it is not possible to prescribe criteria which will specifically fit each situation.

Guard forces are required for all restricted areas. However, the need for guards is roughly in proportion to the scope of activities, the numbers of personnel involved, and the size of the facility concerned. As these factors increase, the safeguards provided by individual employees tend to decrease, resulting in the need for a guard force to control access to the restricted area involved. Guard forces are seldom required at facilities of individual consultants and small laboratories involving only a few individuals. The security interest at such facilities usually consists of documents or materials of such type and amount as to be adequately safeguarded by appropriate depositories and by personal custody of cleared personnel utilizing such matter in the performance of their work.

Stand-by facilities may require guards to control access and protect against malicious or accidental damage when the facilities constitute essential insurance for the continuity of production or service.

It is impractical to guard the entire length of all pipe lines, consequently the emphasis in pipe line protection should be one means for making pipe line repairs as quickly as possible.

The protection of individual wells in a large majority of cases is neither economical nor practical.

Where the nature and scope of the industrial security program of a facility are such as to include a guard force, it constitutes one of the most important single elements in the program. At the same time, the continuing cost of guarding a facility in most cases represents the largest item of security expense. The use and deployment of a guard force should, therefore, be carefully planned and continuously reviewed to the end that the most effective and economical utilization of manpower commensurate with security needs may be obtained.

Due to the widely differing types of situations and extreme range of security interest at facilities, the guard forces requirements, utilization, and deployment at an installation must be locally determined after evaluation of all factors, including the importance, classification, and vulnerability to damage of the data, materials, equipment or activities involved; the arrangement, size, and location of the facility, and the effectiveness of other security measures in effect.

All guards should be investigated and cleared. Guards occupy a position of high trust. By the very nature of their duties and responsibilities in the security program, they may through necessity or the inadvertence of others, come into knowledge and/or custody of vital information, other classified matter, or material of high strategic and/or monetary value. Unquestioned loyalty and integrity is, therefore, an essential requisite for all guards.

If a facility requires the establishment of a guard service, the following elements should be considered.

a. ***Organization***

Guard forces should be organized under the direction of the security director, and operate directly under the supervision of a Chief of Guards. One individual should be placed in charge of each shift of the guards. In small facilities, the Chief of Guards may assume this function on one shift with subordinates on the other shifts. Clear and definite understanding should exist as to seniority and who is in charge of the guard force.

Guards may be organized by:

(1) Fixed post deployment.
(2) Patrol deployment.
(3) Response to calls for assistance.
(4) Any combination of the above three.

A list of telephone numbers for use in emergency should be in guard headquarters. Written records covering all orders and assignments should be maintained.

Guards should be assigned to shifts in accordance with local requirements, but guard shifts should be so scheduled that they will not coincide with employee shifts.

The posts of guards should be varied and they should never know in advance to what post they will be assigned when coming on duty.

Written reports should be required as to guard activities. These should be made up either by the guard himself or by the Chief of Guards, prepared from verbal reports made to him by individual guards.

Guards should definitely understand their relationship to employees. They have certain duties to carry out in respect to employees, but bad employee relationship can result if guards become officious and assume powers which are not rightfully theirs.

Guards who are assigned to fixed posts should have some designated method of securing relief if such is required. Where fixed posts do not permit the guard to move at all, such as guards in watch towers, arrangements should be made so they may leave their posts not less than every two hours.

A simple but effective plan of operation should be worked out for the guard force to meet every foreseeable emergency. Practice alarms (like fire drills) should be run from time to time to test the effectiveness of this plan and the understanding of it by the guard force. Such plans should be particularly designed to prevent a ruse at one point in the facility drawing off the guard and distracting their attention from another section of the facility where unauthorized entry may be made.

b. ***Guard Instructions***

General and special orders should be issued in writing covering the duties of each post and assignment. Such orders should be carefully and clearly worded to include all necessary phases of each assignment. They should be reviewed not less often than monthly to be certain they are currently applicable. Periodic inspections and examinations should be conducted to determine the degree of understanding of and compliance with all orders.

A guard manual or handbook setting forth policies, organization, authority, functions, procedures, and miscellaneous operating information should be prepared and distributed to all members of larger guard forces. Each guard should be held responsible for full knowledge and understanding of its contents.

These instructions will normally cover such duties as enforcement of the pass and identification system, observation of designated perimeter barriers to prevent unauthorized entry, and other duties related to the protection program in general.

c. ***Guard Qualifications***

In order to adequately perform necessary, continuing and emergency functions, guards should

be limited to individuals who meet the qualifications set forth below:

(1) Loyalty.

(2) Within the age limit of 21 to 55 years, inclusive, when providing guard services to restricted areas.

(3) Intelligence.

(4) Physically qualified to perform the required duties.

(5) Dependability.

(6) Cooperativeness.

(7) Exercise good judgment, courage, alertness, tact, self-reliance, of even temper, and have the ability to maintain good performance.

Individuals with military experience usually have the essential qualifications for good guards. In addition, an examination of their discharge papers usually reveals the score the individual received for mental aptitude on his Army General Classification Test. Generally, a score of 100 would indicate sufficient mental aptitude to perform guard duties.

d. *Training*

The extent and type of training for guard forces will vary considerably depending on the importance, vulnerability, size, and other factors affecting a particular installation. However, each member of a guard force should be required to complete a course of basic training and thereafter periodic courses of in-service or advanced training. All such courses should include necessary phases of on-the-job training prior to initial or new assignments and appropriate supervision and follow-through thereafter. Appropriate subjects for inclusion in the various training courses are as follows.

(1) General orientation.

(2) Purposes and principles of the system of security.

(3) Security as applied to the local installation.

(4) Organization of the guard force.

(5) Functions of the guard force.

(6) Specific duties of the individual, including sufficient "breaking-in" training.

(7) Authority of the individual guard.

(8) Guard orders—general and specific.

(9) Discipline.

(10) Employee and public relations.

(11) Instruction in the use, safe practices, and maintenance of sidearms.

(12) Weapons qualification and firing on practice courses.

(13) Self-defense.

(14) Communications facilities and procedures.

(15) Elementary first aid and fire protection.

(16) Operation and care of motor vehicles.

(17) Report writing.

(18) Riot control.

(19) Traffic control.

(20) Operation and use of special equipment.

All personnel of guard forces should be required to undergo periodic in-service training to include necessary review of basic material and such other subjects as may be applicable to the specific installation.

Special and advanced training should be required at all installations where the duties of the guard force are more varied and complex. In such cases, it will be necessary to conduct additional specialized training for selected individuals and supervisory personnel of the guard force.

All guards should receive training in procedures necessary for the implementation of emergency and disaster plans formulated for such facilities. Training should include periodic practice alerts and rehearsals of such procedures. Such training should include coordination with outside agencies which may be called in the event of emergencies beyond the capabilities of local security forces. In most instances, this will involve civil law enforcement agencies.

e. *Guard Weapons*

Guards should be properly armed at all times when on duty. In most cases, the weapons of issue should be .38 caliber revolver as that weapon is in wide usage for police and guard service, and its use would lend to ease in procurement of ammunition and interchangeability of weapons and parts. However, at key posts of critical facilities semiautomatic weapons, riot guns, and other emergency weapons may be provided. Such weapons and ammunition supply should be available at strategic points, properly controlled, and maintained in operating condition for emergency use. All members of the guard force should be legally authorized to carry firearms in the performance of official duties and in the areas where such duties are performed. If guards are armed, the question of bonding should be thoroughly explored by the employer. Guards may be deputized by local police departments to make arrests, if necessary, in the vicinity of the facility.

f. *Guard Uniforms*

Guards should wear a uniform or other means of ready identification when on duty.

g. *Equipment*

All guards should be equipped with a flashlight, police whistle, notebook and billy, in addition to sidearms.

h. *Communications*

Adequate communications are essential to the effective operation of the guard force during normal periods and especially in the event of an emergency or disaster. The type and comprehensiveness of a communications system will vary considerably

depending on the importance, sensitivity, size, location, and other factors affecting a facility.

i. *Supervision*

Supervision of a guard force is necessary to assure the effectiveness of the mechanics of guarding and detecting and taking appropriate action in case of emergency or unusual circumstances. The morale and general efficiency of the individual guard is largely dependent upon the quality of his supervision.

At facilities where guard forces of several men per shift are engaged, full-time personal supervision is needed. The ratio of supervisory personnel to guards at larger facilities and elsewhere, where practicable, should not exceed 1 to 12. Personal supervision should include the following:

(1) Each guard should be inspected by his appropriate supervisor prior to reporting to duty each shift. At such times he should be given any special instructions or orders which may be necessary.

(2) Each guard post, patrol, and other activity should be personally contacted by supervision at least once per shift to determine that personnel and the system in general are functioning properly.

Various means and devices may be successfully utilized as supplements to personal supervision or in the case of small facilities or remote areas, to supplant personal supervision as a means of assuring that necessary areas are patrolled and that other functions are performed. These include the following:

(1) Recorded tour systems, under which guards record their patrols or presence at strategic points throughout an installation by use of portable watch clocks, central watch clock stations, or other similar devices, are effective means of insuring that such points are regularly covered, and have application at most facilities. This system provides an "after the fact" type of supervision.

(2) Supervisory tour systems by which a signal is transmitted to a manned central headquarters at the time the tour station is visited have application at a limited number of the most vital facilities to supplement personal supervision or at facilities with small guard forces, to supplant personal supervision. This system provides instantaneous supervision of the guard, plus a means of detecting interference with his normal activities and a means of initiating an investigation and/or other appropriate action.

All guards should be required to regularly report to headquarters by usual means of communication. The frequency of such reports will vary, depending on a number of factors including the importance of the installation.

Records of tours and reports to headquarters should be carefully checked. Failure on the part of a guard to record a visit at a designated station, to report to headquarters as required, or other deviation from established reporting procedures should be immediately investigated.

j. *The Use of Other Security Elements*

The efficiency and overall effectiveness of the guard force will be increased by the application of such measures as the most effective location of barriers, adequate protective lighting, properly designed guard shelters, use of protective alarm devices where their use is practical, adequate communication facilities, appropriate emergency procedures, etc. The proper application of those measures will help to keep the size of the guard force to a minimum.

k. *Location of Guard Posts*

Local conditions will dictate the number and location of guard posts at each restricted area. During the hours of darkness all guard posts, foot patrols and guard shelters should be located in the darkened areas behind the protective lighting screen. Consideration may be given to providing, where possible, at least one guard post located at some high point within each vital area. This post should be provided with a high caliber rifle, or similar weapon, a manually operated searchlight, and protection from small arms fire.

l. *Guard Shelters*

Guard shelters should be basically designed to provide occasional temporary protection from severe weather. The design should include: space for one guard only; facilities such as heat, ventilation, storage space for essential guard accessories, and lighting which will not expose the guard; good visibility in all direction; windows which can be opened and used as gun ports; provision for adding barricades such as concrete to make the shelter bullet resistant when necessary and providing maximum height barricades. Guard shelters should be painted to render them inconspicuous.

m. *Limitations of Guard Functions*

Guards should have no fire-fighting or other duties. Such emergencies offer an excellent diversion to cover the entrance of a saboteur. Consequently, during such times guards should be more than normally alert in the performance of their guard duties. It cannot be too strongly emphasized that guards are for guard duties and should not be given other functions except in small plants of insufficient size to warrant even one full-time guard.

2. FENCING AND OTHER ANTI-PERSONNEL BARRIERS

Fences and other anti-personnel barriers are the physical media by which restricted areas are physically defined for protection and control.

The fundamental purpose of physical barriers is to deny or impede access to security areas by unauthorized persons. They accomplish this by one or more of the following:

(1) Defining the perimeter of security areas.

(2) Creating a physical and psychological deterrent to innocent entry or to persons attempting or contemplating unauthorized entry of security areas.

(3) Delaying intrusion into security areas, thus making more likely the detection and apprehension of intruders by guard forces.

(4) Facilitating effective and economical utilization of guard forces. In addition, physical barriers serve the purpose of directing the flow of personnel and vehicles through designated portals in a manner which permits efficient operation of the personnel identification and control system.

There are two general types of physical barriers, natural and structural. Natural barriers include rivers, seas, cliffs, canyons or other terrain difficult to traverse. Structural barriers are man-made devices such as fences, walls, floors, roofs, grills, bars, road blocks or other structures which deter penetration. Physical barriers will delay but will not stop a determined intruder. Therefore, such barriers to be more fully effective should be augmented by guard personnel.

Physical barriers which are as manproof as economically feasible should be established around all restricted areas. The type of barrier used should be determined after a study of local conditions. In evaluating the respective merits of chain link fencing and other types of barriers, consideration should be given to the better visibility provided by a chain link fence and the resultant probability of earlier detection by area guards of external approach.

In establishing physical barriers, special consideration must be given so that operating efficiency will not be sacrificed through lack of planning and essential barriers will not be sacrificed for operating expediency.

In some instances, the temporary nature of the security interest makes the construction of costly physical barriers impractical and unjustifiable. In such cases, the security interest must be protected by other means such as additional guard forces, patrols and other compensating protective measures.

In cases of extreme criticality and vulnerability of a facility, it may be desirable to establish two lines of physical barriers at the restricted area perimeter. Such barriers should be separated by not less than 15 feet and not more than 150 feet for optimum protection and control.

The immediate boundaries of a facility should be fenced or posted as is appropriate to establish a legal boundary. If a fence is used, a secondary type such as two or more strands of barbed wire with "no entry" signs attached will suffice. This definitely defines the perimeter, provides a buffer zone, facilitates control and makes accidental intrusion unlikely.

When appropriate, clear zones on both sides of the perimeter barrier of the restricted area should be maintained in order to provide an unobstructed view of the barrier and the ground adjacent thereto and should be kept cleared of material, equipment or other objects which would offer cover or assistance to an individual seeking unauthorized entry.

A barbed wire fence may be appropriate as a part of a restricted area perimeter in extremely rough or steep terrain.

In establishing any perimeter barrier, due consideration must be given to providing emergency entrances and exits in case of fire.

Water approaches to a facility boundary and restricted areas present special security problems. Such areas should be defined by appropriate signs, buoys, booms, etc. Boat patrols may be required at some installations. In inclement weather such patrols cannot provide an adequate degree of protection and must be supplemented by other means such as foot patrols.

Where fences are utilized for the physical barriers of restricted areas, they should meet the following requirements.

(1) Be of chain-link design of not larger than 2-inch square mesh of No. 9 gage or heavier wire. (American wire gage) with twisted and barbed salvage top and bottom.

(2) Eight feet high topped with 3 strands of barbed wire 1 foot high, making a total of 9 feet. Under conditions of national defense emergency, the control of material may make it impossible to obtain this type of fence and other expedients may have to be employed.

(3) Be drawn taut and securely fastened to rigid metal posts set in concrete with additional bracing as necessary at corners and terminals.

(4) Be extended to within 2 inches of firm ground. In some areas, fencing should extend below ground sufficiently to compensate for sandy or shifting soils. Culverts, troughs, etc., should be provided where necessary to permit carry-off of excessive surface drainage and small streams. Such openings, larger than 96 square inches in area, should be provided with physical barriers equivalent in protective capabilities to those of the perimeter barrier and so designed as to minimize impediments to water run-off.

(5) With due consideration to terrain features and building lay-out, be as straight as practicable and, where property lines, location of facility, and

adjacent structures permit, be located within the limits of 50 and 150 feet from the location, building, or object of protection. Generally, the smaller the area the more effectively it can be observed during fog and other inclement weather, thereby affording maximum protection with a minimum of guard personnel.

(6) Be arranged, when appropriate, so that there is at least 20 feet of clearance between perimeter barriers and exterior structures, parking areas, or other natural or cultural features which would offer concealment or assistance to unauthorized access of the area protected. Where due to property lines, the location of a facility, or adjacent structures, this is not possible, perimeter barriers should be increased in height or otherwise designed to compensate for the proximity of such aids to concealment or access.

(7) Where walls, floors, or roofs serve as barriers, they should in general be of such construction and so arranged as to provide uniform protection equivalent to that provided by chain-link fencing as specified. In this connection, windows and other openings in perimeters of restricted areas in any of the following categories should be protected by securely fastened bars, grilles, or other equivalent structural means:

(a) Openings less than 18 feet above uncontrolled ground, roofs, ledges, etc.

(b) Openings less than 14 feet directly or diagonally opposite uncontrolled windows in other walls, fire escapes, roofs, etc.

(c) Openings less than 3 feet from uncontrolled openings in the same wall.

The number of gates or doors in perimeters of restricted areas should be limited to the number necessary for the efficient and safe operation of the facility. Gates and doors not under guard observation or alarm protection should be of such material and installation as will provide protection equivalent to the perimeter barriers of which they are a part.

All means of entry not covered by the above, such as sewers, air ducts, tunnels, etc., which have a minimum dimension of greater than 6 inches and a cross-section area of 96 square inches or more, should have barriers equivalent in protective capabilities to that provided by the perimeter barriers of the area to which they give access.

3. PROTECTIVE LIGHTING

The determination as to the necessity for protective lighting depends on many considerations such as:

(1) The military policy toward blackouts and dimouts.

(2) The location of the facility.

(3) The size, type and character of the facility.

(4) The advantages afforded which may result in a reduction of the number of guards required.

(5) The advantages protective lighting affords in unguarded, isolated facilities by providing an increasing possibility of observation from highways, water approaches, etc., by local law enforcement officials, the general public and periodic car patrols.

(6) The availability of protective lighting materials and equipment.

(7) Management Policy.

Many individuals contend that protective lighting pinpoints critical and vulnerable areas and thus aids a saboteur. It is also contended that in general a trained and properly supervised saboteur already knows, or is familiar with details of the critical and vulnerable area before any attempt at sabotage is made. Experience has indicated that this contention is usually true.

The decision as to whether or not protective lighting should be provided is management's responsibility and is contingent on military policy to some degree.

Generally, protective lighting is inexpensive to maintain and, when properly employed, may reduce the necessity for additional guards and may provide present guards with personal protection by reducing the advantages of cover and surprise by a determined saboteur.

Protective lighting, as a part of the security system against sabotage, espionage, or theft of critical materials, should normally be determined by management to be required only for restricted areas. This does not preclude the use of normal industrial lighting as an aid to the prevention of theft of valuable property, safety or for other reasons.

Protective lighting systems provide a means of continuing, during hours of darkness, a degree of protection of a facility approaching that which is maintained during daylight hours. They serve this purpose by enabling the guards and other employees to observe activities in the area and to take appropriate defensive action, when necessary, and by acting as a psychological deterrent to potential intruders.

There are four types of protective lighting systems:

(1) *Continuous* lighting is the most common protective lighting system. It consists of a series of fixed luminaires arranged to continuously flood a given area with light during hours of darkness.

(2) *Stand-by lighting* is a system wherein the luminaires are not continuously lighted but instead are either automatically or manually turned

on at such times as suspicious activity is detected or surmised by means of guards or alarm systems.

(3) *Movable lighting systems* consist of manually operated, movable searchlights which may be either continuously lighted during hours of darkness or lighted only as needed. These systems will normally be used to supplement either 1 or 2 above.

(4) *Emergency lighting systems* may duplicate any or all of the above systems. Their use is limited to times of power failure or other emergencies which render the normal system inoperative.

Several types of luminaires are adaptable to protective lighting systems. These are:

(1) The reflection type in which a parabolic mirror directs the light as required. They are available in narrow, focused beam, spotlight types and in wide-angle types up to 180°.

(2) Pendant luminaires with a refractory lens designed so as to direct most of the light in the direction needed.

(3) Combinations of types 1 and 2 above.

In most instances the primary source of power for protective lighting will be from public utilities. This may be supplemented by a local secondary supply provided by gasoline or Diesel-driven generators or by battery systems.

Appropriate protective lighting should be employed at all pedestrian and vehicle entrances to restricted areas of all facilities where guards or other personnel are engaged to check identification.

Protective lighting should not be used as a psychological deterrent only. It should be used only where the restricted area perimeter line is under continuous or periodic guard observation, not less frequently than hourly.

Protective lighting may be unnecessary where the restricted area perimeter line is protected by an appropriate central station alarm system.

Those restricted areas located in muncipalities or totally within buildings where dependable street lighting or other functional lighting serves the purpose of protective lighting should not require an independent protective lighting system.

Protective lighting may be desirable for those sensitive areas or structures located within the perimeter of restricted areas which are under specific guard observation. Such areas or structures include underwharf areas, vital buildings, storage areas, and vulnerable control points in communication, power, and water distribution systems.

Under certain circumstances, where restricted areas constitute an extremely attractive target to forces inimical to the national defense, and which for that reason have been located and are operated in a manner to attract a minimum of attention, they may be provided with a protective lighting system which is normally not lighted in order to provide protection in the event of local emergencies or suspicious activity in or near the area. These areas should also have an alarm system to overcome the security limitations of guarding in darkness.

Restricted areas which are of sufficient importance to require manned guard towers, whether continuously or intermittently occupied, normally should be provided with a movable luminary or searchlight system with a light located on each guard tower.

In general, all restricted areas provided with protective lighting should also have an emergency lighting system and a secondary source of power provided by generator equipment or batteries located within the restricted area. The stand-by power source should be adequate to sustain the protective lighting of all vital areas and structures, and should be arranged to go into operation automatically in the event of failure of the primary power. The restricted area should further have generator or battery-powered portable and/or stationary lights at key control points for use of guards in case of a complete failure which renders even the secondary power supply ineffective.

The differences in building arrangements, terrain, atmospheric conditions, and other factors make necessary the design of each lighting system to meet the conditions peculiar to each restricted area. Data are available from manufacturers of protective lighting equipment which will assist the engineers in designing a lighting system. Included among this material are:

(1) Descriptions, characteristics, and specifications of various incandescent, arc, and gaseous discharge lamps.

(2) Lighting patterns of the various luminaires.

(3) Typical lay-outs showing the most efficient lay-out, height, and spacing of equipment.

At fixed luminary installations:

(1) Insofar as possible, the cone of illumination from illuminaires should be directed downward and away from the structure or area protected and away from the guard personnel assigned to such protection. The lighting should be so arranged as to create a minimum of shadows and a minimum of glare in the eyes of guard personnel.

(2) Luminaires for perimeter restricted area fence lighting should be located a sufficient distance within the protected area and above the fence so that the light pattern on the ground will include an area on both the inside and outside of the fence. Generally, the light band should illuminate the restricted area barrier and extend as deep

as possible into the approach area. Adjacent waterways, highways, railroads, residences, etc., may limit the depth of the light band.

Movable luminaires located on guard towers should be so installed that they may be focused in all directions in which the guard is expected to render protective observation. This normally will be a full 360°. They further should be located in a manner which permits the guard to operate the light without increasing his exposure and without deserting his communication facilities or emergency weapons.

The intensity of illumination for protective lighting for fence or other anti-personnel barriers should meet the following requirements:

Location	*Foot candles on horizontal at ground level*
Perimeter of restricted area	0.2
Entrances (vehicular and pedestrian)	1.5
Sensitive inner structures or areas	0.2

Both multiple and series circuits may be utilized to advantage in protective lighting systems, depending upon the type of luminary used and other design features of the system. The circuit should be so arranged that failure of any one lamp will not darken a long section of a restricted area perimeter line or a major segment of a critical or vulnerable position. Connections should be such that normal interruptions caused by overloads, industrial accidents, and building or brush fires will not interrupt the protective system. In addition, restricted areas should have feeder lines located underground, or sufficiently inside the perimeter in the case of overhead wiring, so as to minimize the possibility of sabotage or vandalism of feed lines from outside the perimeter barrier. The design should provide for simplicity and economy in system maintenance and should require a minimum of shut-down for routine repairs, cleaning, and lamp replacement.

4. PROTECTIVE ALARM SYSTEMS

Protective alarm systems provide an electrical and mechanical means of detecting and announcing proximity or intrusion which endangers or may endanger the security of a restricted area, a facility or its components. Protective alarm systems are utilized to accomplish one or more of the following purposes:

(1) To permit more economical and efficient use of manpower by substitution of mobile responding guard units for larger numbers of fixed guards and/or patrols.

(2) To take the place of other necessary elements of physical security which cannot be used because of building lay-out, safety regulations, operating requirements, appearance, cost, or other reasons.

(3) To provide additional controls at vital areas as insurance against human or mechanical failure.

Generally, it may be stated that there are two types of alarm systems:

(1) A central station alarm system is one in which the operation of electrical protection circuits and devices are automatically signalled to a central station which has trained guards and operators in attendance at all times. The central station monitors the signal end of the alarm system, provides the response to a signal, and supervises the functioning of the system.

(2) A local alarm system is one in which the protective circuits and devices are connected to a visual and/or audible signal element which is located at or in the immediate vicinity of the protected facility or component, and which is responded to by guard personnel in the immediate vicinity.

There is on the market a variety of alarm equipment based on different principles of operation and designed to meet various requirements. There are, however, four fundamental elements required in all alarm systems. These elements are:

(1) A detection device or series of such devices. Most common among these are:

(a) Foils, screens and traps which are damaged or disturbed by penetration. (Usually used for protection of doors, windows, ducts, and non-substantial walls or partitions.)

(b) Photoelectric systems, whereby interruption of a virtually invisible beam of light is detected.

(c) Electromagnetic wave or electronic system whereby entrance of an intruder into the field of the system is detected.

(d) Microphonic devices which detect sound and vibration.

(e) Pneumatic detectors of various types which serve the same purpose as mechanical and electrical detectors.

(f) Thermal detectors, actuated by exceeding a predetermined temperature limit or rate of rise.

(2) Electrical or electronic circuits for transmitting signals from the protected area to the signal apparatus.

(3) An alarm or signal apparatus which will announce by audible and/or visual means any activity which the system is designed to detect.

(4) Electronic apparatus which provides visual means of observing activity from a different and remote location.

The Underwriters' Laboratories, Inc., have established Grade A and Grade B classifications for both central station and local alarm systems. Details of requirements for each type and grade of alarm system are set forth in Underwriters' Laboratories, Inc., publications "Standard for Central Station Burglar Alarm Systems (100)," "Standard for Local Burglar Alarm Systems (101)," and "Standard for Installation, Classification, and Certification of Burglar Alarm Systems (102)."*

The use of alarms in the protective program of a restricted area or facility may be required in certain instances because of the critical importance of the area or the facility and in other instances, because of situations and conditions pertaining to the location and/or the lay-out of the area or facility. In some instances, their use may be justified as a more economical and efficient substitute for other necessary protective elements. In determining whether the use of alarms in a restricted area's or a facility's protective program is essential or advisable, the various conditions and situations peculiar to the restricted area or facility will, of course, affect the ultimate decision. However, in general, the following criteria should form the basis for a determination by management of the use of alarms:

(1) The critical importance and vulnerability of certain restricted areas or facilities requires the additional control and insurance against human or mechanical failure which is provided by alarm systems. In this group are:

(a) Restricted areas or facilities which, because of a concentration of vital components, materials, or data, are attractive, high-priority targets for sabotage, theft, espionage, or other criminal acts.

(b) Critical processes and process controls.

(c) Very important restricted areas or facilities where it is desirable to have admission controlled by both guards and operational employees, or where it is desirable for operators to deny access to guards.

(2) In certain cases due to restrictions imposed by location, lay-out, or construction, alarms are necessary to take the place of the more usual protective elements such as fences, lighting, patrols, etc. Included in this group are:

(a) Restricted areas or facilities which because of proximity to adjacent structures, activities, or property lines, require the use of alarms in lieu of physical barriers to limited or exclusion areas.

(b) Restricted areas or facilities which are difficult or impossible to effectively guard due to terrain conditions, personnel hazards, or atmospheric conditions and where other types of protection are not effective or practicable.

(c) Restricted areas or facilities, or components thereof which are small or remote areas requiring more than safe and lock protection but not justifying a full-time guard.

(3) Alarm systems, because of their cost, are justified only where their use results in a commensurate reduction or replacement of other necessary protective elements without loss of protective effectiveness. The objective of such use, in most instances, is to reduce the number of guards otherwise required. In determining the advisability of substituting alarms for other protective elements, a careful comparison of relative costs is essential. This should include consideration of the initial cost of the system as well as recurring service and maintenance charges. In this connection, it should be borne in mind that alarm systems have little salvage value and consequently the longevity of the activity being protected is an important consideration.

To afford the required degree of protection and be acceptable as a protective unit, alarm installations should meet the following requirements:

(a) The system should be so designed that the interval of time between the detection of activity and the achievement of the objective of such activity is sufficient to permit the application of necessary countermeasures.

(b) Central stations systems should be specified for all locations where guards are not continually in the immediate vicinity to pick up a local alarm signal and make adequate response.

(c) All systems, materials, and equipment should meet the Underwriters Laboratories standards where applicable for the purpose for which it is used.

(d) All installations should be made in accordance with accepted Underwriters' Laboratories standards for burglar alarm systems.

Protective alarm systems are designed to augment the guard force and not replace it.

The advice of a competent engineer from a reputable firm dealing in protective devices and signal alarms should be obtained when considering protective alarm protection.

5. PROTECTIVE COMMUNICATION SYSTEMS

(1) Provide the means for expeditious transmission of reports and instructions between guard headquarters, guard posts, and guard patrols both as a matter of routine and as a matter of emergency necessity.

(2) Facilitate the integration and coordination of the guarding function.

(3) Facilitate the efficient and economical utilization of guard forces.

* See Bibliography

(4) Insure expeditious transmission of requests for assistance to outside sources in the event of an emergency beyond the capabilities of a guard force.

(5) Provide for the transmittal of alarm signals to facility guards or to outside sources of response.

Communications systems, for the purpose of this manual include:

(1) Facilities for local exchange and commercial toll telephone service.

(2) Intraplant, interplant, and interoffice telephone systems, with or without switching equipment, utilizing rented circuits and equipment, but not interconnected with facilities for commercial exchange or toll telephone service.

(3) Radiotelegraph and radio telephone facilities for either point-to-point or mobile communications service.

(4) Telegraph and teletype facilities for either commercial service or private line operation.

(5) Central station supervisor automatic alarms.

(6) All other reliable means of electrically or electronically transmitting and receiving a signal, message, or alarms which will be understood as such.

Interior communications are considered to be two-way communications for the exchange of information between two or more points within a restricted area or facility; and, also, one-way communications for the transmission of alarm signals from one or more other locations within the restricted area or facility.

Exterior communications are considered to be two-way communications between a restriced area or facility and an exterior point or points from which assistance may reasonably be expected in the event of an emergency, and for which contingency emergency plans have been formulated.

The types of communication systems utilized and their comprehensiveness will of necessity vary with the criticality, vulnerability, size, location, and other factors affecting a specific restricted area or facility and must be largely subject to local determination. The following general requirements should be met:

(1) At least two systems of exterior communication, one of which should be radio with either an independent or an emergency source of power.

(2) At least two systems of interior communication covering all important fixed areas, of which one system should have an independent power source.

(3) A system of radio communication with and between all necessary motor patrols with each fixed and portable ground station provided with either an independent or an emergency source of power.

(4) A separate warning and alarm system to alert personnel in the event of enemy attack.

Frequent and regular periodic inspections and tests of all communication equipment and circuits should be conducted to insure that they are in proper operating condition. Tests should be conducted at regular intervals under simulated emergency conditions.

Communication centers are very important units of the restricted areas or facilities which they serve and should be safeguarded accordingly.

6. FIRE PROTECTION

Fire is the single greatest destroyer of property. A substantial fire risk is inherent in practically all forms of the petroleum and gas industries. Even in World War II, when tremendous emphasis was placed on keeping systems or facilities operating, fire did tremendous damage. Today fire continues its ravage of petroleum and gas properties. Only recently fire destroyed a petroleum facility. Strangely enough, the source of the fire was one well known to fire prevention engineers and one for which recognized protective devices were readily available. The facility simply did not do an obvious fire protection job.

Most fires and explosions are preventable. The major reasons why fire prevention programs are not fully exploited in all facilities are probably the following:

(1) Personal fire experience is too thinly spread to have much educational value.

(2) Fire protection in any system or facility starts with the conviction that production or service capacity is worth more than insurance dollars. Fire protection buys *time* that dollars cannot buy.

The mechanics of fire prevention and control comprise a library full of standard texts, formulae and tables. Only the experienced professional fire protection engineer can be expected to understand these problems and employ effective measures. No attempt will be made in this set of principles to give specific advice on technical matters as they apply to a particular facility. The advice of an expert on fire protection should be sought if an expert in this field is not already a part of the facility staff.

In general, however, interruptions in production or service and destruction from fire can be prevented through good housekeeping, division of values, adequate physical barriers to prevent spread of fire, the elimination of fire causes, ample fire first-aid, and manual and automatic fire control and extinguishing equipment where products or process materials are combustible. In addition, the organization of a system or facility fire brigade, the establishment of a fire alarm service and the

assurance of thoroughly reliable and adequate water supply are essential.

Real fire protection starts with a survey of the system or facility and with realistic solutions of the so-called "fire problems." A fire problem is a hypothetical fire that starts under adverse conditions in time and place within the system or facility. The question is how can it be stopped before it gets out of hand. The solution of such a problem is not theory or guesswork, but the application of expert knowledge to a particular task. Management may obtain an impressive picture of the difficulties encountered in working out such problems by walking through a facility alone in the dead of night or on a Sunday. Management should stop and think of what would happen if and when an accidental or malicious fire got under way in the system or facility. How long would it be before someone found it? How would the finder report it? Who would respond? How would they get the alarm? Where would they connect their hoses? How long would all this take? And during all the time, how fast would the fire be getting under way? The answering of problems such as these points the road to adequate system and facility protection.

The fire hazards created by normal production or service methods are increased in time of alert or actual hostilities by risks arising out of the national defense emergency:

(1) The pressure to get out more work creates conditions that breed fires and make them spread. Taking chances with critical systems and facilities is not only bad business judgment but bad defense planning.

(2) Fire has always been the favorite tool of the saboteur. Time delay ignition devices give him a chance to escape. The destruction that follows hides his tracks. In addition to starting a fire in a vulnerable spot, the saboteur may effectively sabotage fire prevention devices. The saboteur counts on the weaknesses of the system or facility fire protection measures for his success. Management of a critical system or facility must assume that the system or facility may be a target for sabotage and must realize that advice is needed from experts in fire protection. Fire protection measures visualized by the average system or facility operator will not suffice. It is not that the saboteur is smarter than the average system or facility operator, but in such a case the saboteur is a specialist working against an amateur.

(3) Fire protection planning must also take cognizance of the additional threat created by the possibility of direct enemy action. This phase of fire protection is discussed under "Civil Defense Aspects."

No campaign of fire protection may succeed without the complete cooperation of all system and facility employees. Fire protection needs the help of every workman in the system or facility. The idea must be sold and interest maintained. One absolute requisite of employee participation is constant and free contact between all employees and the fire protection force.

The following check list is offered for use in reviewing fire protection measures at all facilities.

(1) Housekeeping and elimination of potential fire hazards.

(2) Proper storage of combustible materials.

(3) Selection of proper fire-fighting equipment for various types of fire hazards and correct location of such equipment.

(4) Regularly scheduled inspection of equipment by qualified personnel to determine if it is in good operating condition.

(5) Employees trained in use of equipment and fully aware of their responsibilities in case of fire.

(6) Arrangements with local fire departments to assist when needed—special training required for electrical fires.

Most large organizations have fire protection procedures and regulations designed to meet their specific requirements. These regulations should be continuously reviewed and revised as necessary.

Fire losses are serious under normal conditions. Such losses are of much more concern under emergency conditions.

References:

Handbook of Fire Protection (Crosby-Fiske Forester). (59) *

Training Manual for Auxiliary Firemen (National Fire Protection Assn.). (95) *

Fire Defense (National Fire Protection Assn.). (55) *

7. SAFETY

In addition to the humanitarian aspect, injuries to personnel result in serious delays in production, destroy morale, and are expensive in time, money and man-power. The magnitude of the accident problem has demanded aggressive organized effort. Accident prevention authorities, such as the National Safety Council and compensation insurers, have vigorously promoted programs to control and reduce personal injuries.

Accident prevention work is essentially a simple and understandable procedure. Most accidental injuries result from two causes:

a. The lack of effective administration of the safety program and the violation of commonly accepted safe practice rules.

b. Exposure to mechanical or physical hazards.

* See Bibliography

Accordingly, accident prevention is designed to eliminate or reduce exposure from these two hazards by means of employee indoctrination and the employment of physical safeguards.

The great majority of injuries in the petroleum and gas industries occur because employees violate common accident rules or assume unwarranted personal risks. Mechanical safeguarding of physical hazards, while necessary and important, can accomplish only a small degree of personal injury reduction, unless it is a part of a constant campaign aimed at inspiring the individual to safeguard his own personal safety. In any safety program, aggressive efforts must be made to devise practical methods of creating safe working habits on the part of all employees, and a positive will to abide by prescribed safety procedures. The maintenance of such a specific campaign becomes the primary safety activity of management. Techniques and methods for this type of campaign may be found in the literature of many associations and are made available to management by compensation insurance companies, State Labor Departments and the National Safety Council.

For example, accident prevention is a well-organized and active force in the petroleum industry. Working through the American Petroleum Institute, the industry's safety engineers and supervisors have prepared guides to safe practices in numerous occupations. These recommended guides are available as API Accident Prevention Manuals:

No. 1—Cleaning Petroleum Storage Tanks

Section A—Crude Oil and Unfinished Products Tanks

Section B—Gasoline Tanks

No. 4—Organization for Accident Prevention

No. 5—Operation of Service Stations

No. 6—Precautions in Well Pulling

No. 7—Precautions for Workers on Construction and Maintenance of Refinery Equipment

No. 8—Bulk-Plant Operation and Delivery of Products

No. 9—Precautions for Oil-Field Work

No. 10 Rotary Drilling

No. 11—Safe Transportation of Petroleum Products by Tank Trucks

No. 12—Loading Tank Cars (Gasoline)

No. 13.—Cleaning Mobile Tanks for the Transportation of Flammable Liquids (Section A—Tank Vehicles)

The most careful worker is nevertheless likely to sustain injury if he is exposed to hazard without adequate personal protective equipment or physical safeguards while engaged in an operation which requires such types of protection. In a system or facility which is properly organized for accident prevention, guarding of hazards by mechanical devices becomes a matter of routine. Buildings and other structures are designed for safety; dangerous moving parts of machines, tools and other mechanical equipment are guarded; safe housekeeping is maintained; devices and techniques especially designed to permit safe operation under all conditions are employed. The designer builds in, or purchases equipment having safety devices which meet the standards of the American Standards Association, National Safety Council, or other recognized organizations.

Safety organization centers around a security director, a safety director, safety inspector and safety committee. The security director and the safety director as the direct representatives of management plan and direct all safety activities and are responsible to management for the effective functioning of the safety program. Safety inspectors survey structures, yards, storage spaces, machines, tools, equipment, materials, safety appliances and equipment, and safe work performances; they report their findings and recommendations, or if necessary, correct unsafe conditions and systems on the spot. They also investigate accidents, prepare records and assist generally in safety work.

The Safety Committee serves as a clearing house and forum, considering:

a. The program of safety works;

b. Recommendations from all sources;

c. Accident investigations;

d. The quality of safety work by all participants in the program;

e. Educational and promotional activities;

f. The correction of outstanding mechanical and physical causes of accidents; and

g. Increased risks in emergencies.

In times of emergency, when production is being raised, the safety problem becomes more acute because of:

a. The employment of new and untrained people.

b. Obsolete equipment.

c. New processes.

d. Substitute materials.

e. Overloaded equipment.

This means that the maintenance of an adequate safety program should become a primary activity of each business. All systems and facilities which have not already done so should expand their safety program to include:

a. An effective safety organization under existing conditions and the conditions that may reasonably be expected during an emergency or disaster.

b. An intensive education program to establish safe employee working habits and safety thinking.

c. Intensive supervision of personnel, premises, processes and production.

d. Disciplinary control of unsafe working practices of employees.

e. Maximum use of proper protective equipment and clothing.

f. Special provision for guarding against physical and mechanical exposures.

g. Adequate first aid and medical facilities.

h. Accident records sufficient to evaluate the effectiveness of the program and the progress made.

i. More frequent inspections.

If both management and employees work wholeheartedly together in the system or facility safety program, the results will be clearly apparent in the reduction of personal injury and the consequent increase in production.

8. MISCELLANEOUS CONSIDERATIONS

a. *Truck Control*

A definite system should be in use to limit and control the movement of trucks and other goods' conveyances into and out of the facility area. Insofar as possible, loading and unloading platforms should be located outside restricted areas.

All trucks and conveyances should be required to enter a restricted area through a service gate manned by guards. Truck drivers and helpers, and vehicle contents should be carefully examined. The guard check at truck entrances should cover both incoming and outgoing vehicles and should include:

(1) Appropriate entries on truck register, including: registration of truck, name of truck owner, signatures of driver and helper, description of load, and date and time of entrance and departure;

(2) Identification of driver and helper, including proof of affiliation with company owning truck or conveyance.

(3) Check of vehicle operators' licenses of driver and helper.

(4) Examination of truck or other conveyance for detection of explosives, incendiary devices or other hazardous items.

Identification badges should be issued to truck drivers and helpers who have been properly identified and registered. Such badges should permit only limited access to specific loading and unloading areas.

Incoming trucks should be kept to that minimum which is essential for the efficient operation of the facilities, and vehicle escorts should be provided if vehicles are permitted access to restricted areas.

Guard supervision of loading and unloading operations should be strictly adhered to ascertain that unauthorized goods or people do not enter or leave the facility via trucks or other conveyances.

b. *Railroad Car Control*

The movement of railroad cars into and out of restricted areas should be so supervised as to prevent the entry of unauthorized personnel or goods.

All railroad entrances to restricted areas should be controlled by locked gates when not in use and should be under guard supervision when either unlocked or opened for passage of railroad cars.

Insofar as possible, loading and unloading railroad car platforms should be located outside restricted areas.

Before entry to the restricted area, all railroad cars should be inspected to prevent unauthorized persons entering the area. The contents of railroad cars should be carefully inspected to prevent the conveyance into the restricted area of explosives or incendiary devices.

Where railroad cooperation can be secured, and it does not materially interfere with efficient facility operation, railroad switching should be confined to daylight hours.

The numbers of the seals of all sealed railroad cars should be checked immediately upon arrival at the facility against the list of seal numbers which should be requested from the shipper. Broken seals or seal numbers not in accordance with advice from the shipper warrant immediate investigation.

c. *Container Control*

Management of each facility should consider establishing a definite system for the control of containers entering or leaving the restricted area. Such control should be desirable as an effective means of minimizing property loss and preventing possible sabotage or espionage.

No containers or packages, except lunch boxes, should be permitted to be brought into the restricted area by employees or others unless they are opened by members of the guard force and thoroughly inspected. Employee lunch boxes should be spot checked from time-to-time.

As a means of safeguarding essential vital information and production tools and equipment, inspection of all restricted area outgoing packages is desirable. In lieu of 100% inspection, frequent unannounced spot checks should be considered.

Empty containers which are to be filled with products that are important to the national defense effort should be inspected immediately prior to filling.

Employees in container storage areas should be so educated that it is second nature for them

when coming on shift, to look for any signs of disturbance or tampering with containers.

d. *Vehicle Parking Areas*

Normally, employees and visitors should not be permitted to park their automobiles within the restricted area. If it is found impractical for all cars to be parked outside of the restricted area, then only employees should be allowed to park within the enclosure. In case of interior restricted area parking, the parking area should be located away from important processes and separately fenced in such a manner that occupants of automobiles must pass through a pedestrian gate before entering the facility.

e. *Power Supply*

Protection of on-the-premises power generating stations and substations should be provided commensurate with their importance to the continued production of facilities' critical items and their susceptibility to sabotage.

The facilities' own power generating units should be established as part of a restricted area or a separate restricted area and only authorized personnel should be permitted access thereto.

Substations on the facility premises, whether owned by the facility or by a public utility company, which supply all of the electric energy used at the facility should also be included in a restricted area or a separate restricted area and only accessible to authorized personnel. When a facility's production is dependent on electric energy, the substations are more critical than individual transformers and should receive protection equivalent to their importance. If the substation is off-site, it should be given protection equal to that of restricted areas within the facility's perimeter. If the off-site substation is owned by a public utility company, officials of that company should be encouraged to properly protect the substation.

The electric power supply should be ample to provide for a reasonable reserve beyond full load demands.

f. *Transformer Installations*

Transformer installations, because of their importance to continuity of production or service, are especially vulnerable to sabotage and their protection should be carefully studied and all reasonable methods of protection applied.

Transformer installations located on a facility's premises should be included in restricted areas, or in separate restricted areas, should be fenced or screened and openings therein locked, and should be included in the itinerary of the guard patrol. Buildings in which transformers are located should be locked and only authorized personnel permitted entry.

Transformer enclosures should be lighted at night unless complete darkness is required to prevent detection of location.

Transformers are vulnerable to rifle fire, and when practicable, should be adequately shielded by sand bagging or other protective measure when required. When enclosed in buildings or shielded, adequate ventilation should be provided.

Transformer enclosures should be kept free of debris, weeds and grass. Large transformers should be equipped with electric alarm pressure and temperature gauges to give warning of an injurious condition within the transformer.

Oil filled transformers within buildings should be in safe locations, should be well drained and provided with curbed pits for the collection of oil. Such transformer sites should be provided with a foam fire extinguisher or other suitable means of sufficient capacity to control an oil fire originating thereat. Oil filled transformers outside should be at sufficient distances from buildings to minimize damage to the facility in the event of fire. Patrols should be on the alert for oil losses resulting from rifle fire and other causes.

Pole transformers located on the poles near the property lines or within the facility area should be under guard surveillance and their security checked by frequent patrols.

Transformers having a non-combustible dielectric may be located at almost any convenient place within the facility property provided they are protected against malicious tampering and mechanical injury.

g. *Electric Power Transmission*

Power lines, power terminals, and power switches and controls located within the facility perimeter should be provided adequate protection to assure the continuous and uninterrupted flow of electric energy to protect the plant.

The main switches, power terminals, and power controls should be located in restricted areas and included in the same protection plans as transformers and electric power substations since they are usually at the same location. Secondary switches located in operating areas should be readily accessible so that power can be shut off in an emergency.

Distribution lines should be properly insulated and supported. When justified economically, underground power lines should be employed.

h. *Communication Centers and Equipment*

The communication center and allied communication equipment which is essential to the operation of the facility should be adequately protected to prevent sabotage and tampering.

The telephone exchange, the teletype and/or the short wave radio room and such other control centers as the guard headquarters should be restricted areas. When not individually manned, each such installation should be securely locked or guarded. Dispersion within the facility of the several means of communication, such as teletype, telephone switchboard, public address system, and short wave radio may be advisable to afford adequate protection.

Frequently, communication installation areas are used individually or jointly as an emergency control center; as such, they are of the most vital importance and should be adequately protected. When an emergency control station is established in a shelter area for use in case of air attack, its communication equipment should be a restricted area and protected against tampering or unauthorized entry.

i. ***Valves, Regulators and Regulation Stations***

Main control valves, regulation stations and regulators should be protected to prevent tampering and unauthorized manipulation, but should be accessible to authorized personnel for emergency use.

Main shut-off and control valves locations should be restricted areas and enclosed. If exposed such valves should be locked in the position required for normal operations. Manholes and pits containing control valves should be secured by covers locked in place. Equipment or control valves with electric signalling devices should be considered as an additional means of protection against tampering.

Gas valves and regulators should be within a noncombustible locked enclosure, adequately ventilated to prevent accumulation of gas and provided with vapor-proof or explosion-proof electric equipment. Gas valves used infrequently should be locked or sealed. Guards should check the enclosures and the valves and regulators periodically.

j. ***Water Tanks and Pumps***

Water tanks, water pumps and allied equipment essential to the operation and production of the facility should be afforded adequate protection to prevent curtailment, contamination or damage of the water supply.

Water tanks, pumping stations, pumps, and equipment should be within restricted areas and checked frequently by guards. Water tanks, pumps and equipment preferably should have an electric supervision system to check water supply and indicate water failure.

Elevated water tanks should be fenced and the gates locked. Roof tanks should be secured by screening or locked roof doors.

Pumping equipment located in a building or room should be protected by having all doors and windows of the enclosure adequately barred or locked. Pumps should have more than a single source of power for their operation.

k. ***Gas and Oil Fields***

Regular field operating personnel, to the extent that is necessary to obtain reasonable protection by this means, should be armed.

Printed lists and locations of fire fighting and emergency equipment should be compiled for each operating area. Each operator should have one of these lists.

A directory should be maintained of trained oil and gas well fire fighters, equipment and other essential information.

Insofar as practical, each operating company should keep its fire fighting equipment, repair equipment and supplies in or near these critical producing areas.

Where no operating personnel is present in the oil fields at night, special arrangements should be made for the prompt provision of fire fighters when needed.

Special protective committees should be formed from among the operators in a given critical area. The objective of these committees should be the security of the maximum protection possible on a mutually cooperative basis. These committees should maintain close contact with the military and other organizations which may be concerned in the event of a critical situation.

Emergency protective equipment, which in case of sabotage of "Christmas Trees" would shut off flow of wells, such as stream chokes installed with casing packer, should be used insofar as they are economically and physically practical. Some special situations may warrant the sandbagging of "Christmas Trees" or similar protective measures, such as: area patrols, or armed guards.

l. ***Transportation of Petroleum Products***

Petroleum products shipped in bulk through intermediate distribution points should be tested in laboratories at such points at that time in their handling which will most effectively detect malicious contamination.

As is the general practice in the industry the interior of all containers and tank cars and ship's tanks should be inspected before loading.

All loaded railroad cars should be sealed with numbered car seals and advice sent to the consignee of the seal numbers so that he can verify them on arrival of shipment. On especially vital shipmens by rail the cooperation of the railroads should be solicited to give special protection to the shipment enroute.

Tank wagons used for handling products in the category dealt with here should be protected against tampering when they are garaged. The tanks of these tank wagons should be inspected before filling. After filling the tanks should be sealed. The tank driver should never be permitted to leave a full tank wagon until its complete load has been delivered.

To the extent that it is possible, trucks carrying truck loads of products should be sealed and the seals checked at destination. Reloading of full truck loads enroute should not be permitted.

The tanks on tankers and barges containing products in this category dealt with here should be sealed after filling and the seals checked before unloading. Where barges deliver a part cargo one day, the remainder the next, and have no special protection during the night, their tanks should be sealed between deliveries.

m. *Dispersion of Production*

Dispersion is considered one of the most effective means of reducing the vulnerability of production facilities to enemy attack. It consists in employing the simple military measure of using space for defense. Selection of dispersed sites—even a few miles apart—for new or expanding facilities tends to create a multiplicity of targets and thus reduces the vulnerability of any one concentration.

Dispersal of production processes even within the same plant should be considered as one means of assuring continued production despite some damage at a single location. The principle should be adapted to the individual characteristics of the industry or the particular facility. When production or service is dependent on a limited number of specialized processes, equipment, materials, etc., management should consider the possibility of isolating individual units or providing alternate units, so that damage to one portion of the plant would not cripple the operation of the entire facility or system.

n. *Facility Locations*

When new plants or major expansions are contemplated for purchase or construction, in addition to economic factors normally influencing site selection, important consideration should be given to security of the location from attack.

A new facility should be located a sufficient distance from any densely populated or highly industrialized section of an urban area or from any major military installation. This distance provides relative security against atomic weapons; yet allows location within the metropolitan marketing areas. Management should consult the industrial dispersion committee in the area in which it plans to locate for advice on availability of suitable sites meeting national dispersion standards.

o. *Emergency Shut-Down Procedures*

Emergency shut-down procedures should be developed as a means of minimizing damage to process and production equipment, special tools and instruments easily susceptible to irreparable damage. Such procedures should be tested for adequacy and effectiveness.

Machine and process operators should be made responsible for assuring that production or service equipment is properly shut off when the "take cover" signal is given on the approach of imminent danger.

Safeguarding of certain equipment may require more complicated procedures than a full shutdown. It may be necessary to keep certain auxiliary protective equipment in operation, or it may be necessary to cover or remove small tools and delicate instruments to safeguard them against flying debris and dust.

The closing down of utilities should be on a very selective basis because of their vital contribution to the operation of the facility under emergency conditions. Water may be required in some mains for fire fighting and electricity may be required to run emergency lighting and ventilating equipment. Normally, water and electricity should be shut off at individual meters and valves rather than at the incoming mains.

After properly closing down or safeguarding machinery, equipment and utilities, facility personnel should report to their assigned emergency duty stations with the facility protection organization or proceed to the shelter areas.

D. PASSIVE DEFENSE AGAINST DIRECT ENEMY ATTACK

Passive defense measures embrace those precautions taken in connection with the construction, design, and layout of buildings which will afford to personnel and equipment protection against such destructive forces as blast, fragmentation, radiation and other effects of enemy air attack. These measures include dispersion, duplication, camouflage, personnel shelters, underground construction and similar measures designed to minimize casualities and damage to equipment. They vary in degree of protection and are necessarily limited by the importance of the facility and economic factors. Studies of the system or facility will determine the items which are most vulnerable to various types of attack.

1. BLAST BARRIERS

Consideration should be given to the use of protective barriers around vital processing equip-

ment, pumping, compressor and regulating stations.

There are two general approaches to the blast barrier problem. If fireproof, reinforced concrete or steel frame buildings are available in the required locations, advantage should be taken of the protection against blast and radiation that can be provided in selected areas of such buildings. If no such buildings are available, protective blast barriers of appropriate materials may be constructed around the vital equipment, etc.

2. CAMOUFLAGE

The effectiveness of camouflage has been greatly reduced by radar technique so that its value as a protective measure is questionable, particularly in view of the cost.

In isolated cases, where camouflage is deemed necessary by defense authorities, detailed technical advice will be furnished by military experts. Camouflage is a highly specialized subject which should not be undertaken except on express direction of military authority.

3. BLACKOUTS AND DIMOUTS

In view of the effectiveness of radar and the hazards involved in operating under blackout conditions, the benefits of blackout in the petroleum and gas industries are probably off-set by the hazards involved.

Military policy will govern the use of blackouts and dimouts.

4. BOMB SHELTERS

Shelter areas should be designated within existing structures to afford the best available protection. These areas should be readily accessible and clearly marked. During an attack, it is important that the number of employees who are required to remain at their station be kept at a minimum.

In selecting shelters, the following should be considered:

(a) Structural adequacy;
(b) The number of persons to be sheltered;
(c) Readily accessible entrances and exits;
(d) Improvised sanitary accommodations; and
(e) Facilities for heat, light, etc.

Sources of danger such as the following should be carefully avoided:

(a) Excessive overhead loads of machinery or other heavy objects.

(b) Presence of water and gas mains, sewage systems, steam pipes, or pipes carrying refrigerants or noxious chemicals.

(c) Nearby storage of flammable or corrosive liquids.

(d) Multiple electric conduits and switchboards.

Assembly of large groups should be avoided and, if practicable, shelters should be dispersed.

E. ACTIVE MEASURES MINIMIZING EFFECTS OF ENEMY ATTACK

The responsibility for active defense against overt enemy attack rests with the military. However, it must be assumed that some portion of enemy attacks will get through these defenses. Under such circumstances, properly planned and implemented active measures minimizing the effects of enemy attack will reduce losses to personnel and equipment and provide for more effective restoration of production or service.

1. CIVIL DEFENSE ASPECTS

An essential part of any protective program are measures to minimize the effects of enemy attack. These measures are similar to these Civil Defense Services now being established in communities throughout the country. It should be recognized that in a large scale disaster, the demands upon civil defense and other community services will be so great that each petroleum and gas system and facility must be prepared to do its utmost to protect itself. Each system and facility, therefore, should establish a self-protection program with the aim of reducing losses to personnel and equipment in the event of enemy attack. In view of this, petroleum and gas system employees should not be committed other than in the capacity of consultants, to outside civil defense organizations unless their services are not required in the self-protection program. Civil Defense starts in each system or facility and outside help should be summoned only when the disaster is beyond the capabilities of an individual system or facility. When outside assistance is called, it should operate under the direction and supervision of qualified petroleum or gas system employees.

These measures to deal with emergency situations can be established in all petroleum and gas installations regardless of size or type at no substantial cost and require no additional personnel. Present personnel are formed into groups and trained to perform under the direction of the security director in specialized services, such as fire-fighting, engineering services, rescues, and first-aid to safeguard the facility and its occupants in time of disaster.

a. *Centralizing Control*

To use effectively all resources at his command during an emergency, the security director must

be acquainted with the overall situation, coordinate the activities of the different services, and check results. The mechanism he uses for this purpose is the control system operating from a central room. It should function during an enemy attack or a peacetime disaster such as fire or explosion, when damage occurs simultaneously at several points. Even a small facility should have a control system.

One of the requirements for control is a communications system linking the control room with various areas of the plant. As pointed out in the section on Communications provisions should be made for alternate means of communication in an emergency.

The security director and his staff should go to the control room at the first warning of an emergency. It is the focal point of intelligence and command. Here, reports are received, requests for assistance are evaluated, strategy is determined and orders are issued. The control room also serves as a contact point with the local civil defense organization and with neighboring facilities with which a mutual aid agreement has been established.

If at all possible, the control room should be established in a well protected area, preferably underground, and it should also be protected against sabotage. It should contain system and facility maps and charts so that damaged areas can be readily identified and marked. There should be an alternate location for an emergency control center to function in the event of damage to the regular control center.

In a large system or facility, the Security Director's staff should comprise deputy directors and heads of the engineering, fire, warden, guards, health and welfare services. Other control room personnel should include telephone operators, radio operators, messengers and a map clerk.

b. ***Air Raid Warning System***

Timely warning of an air attack is vital to control. Anticipation permits movement of employees to shelter areas, shutting down of equipment, where feasible, to reduce hazard to personnel and chance of damage and assembly of rescue, medical and fire groups. The system or facility warning signal should be given by the control center on receipt of warning from the Air Defense or Civil Defense Headquarters. The security director should establish a working liaison with his local Civil Defense Headquarters for purposes of receiving such warning and for any other matters concerning a warning and control system.

c. ***Protective Services***

In general, your civil defense protective services should be organized and trained to:

(a) Direct personnel to shelter
(b) Prevent panic
(c) Extinguish fires before they become large
(d) Rescue trapped personnel
(e) Render first-aid and hospitalize casualties
(f) Provide emergency food and shelter
(g) Repair utilities, such as water or power
(h) Repair transportation and communications facilities
(i) Protect lives, property, productive capacity and records and maintain morale.

d. ***Fire Services***

Fire is the chief hazard to petroleum and gas systems and facilities even in peacetime. This hazard is greatly intensified in an emergency period. Fire protection has already been discussed earlier and it is only intended here to mention that organizing of groups for fire-fighting is probably the most important step to be taken in preparing for possible disaster. The functions to be covered include:

(a) Fire prevention
(b) Inspection for fire hazards
(c) Taking immediate steps to extinguish fires and holding down spread
(d) Rescue from fires
(e) Requesting help of local fire departments

e. ***Health Services***

The health services may have to operate against great odds. Even under normal conditions the scarcity of professional people in the health field is a serious problem. This scarcity will become more acute in the emergency as trained personnel are taken into the Armed Services. In view of this, all systems and facilities should organize their own health services and integrate them with the local civil defense organizations. In large systems and facilities there should be a full-fledged health service, consisting of a medical director, nurses and a panel of doctors on call. This staff could be adapted for major disasters by augmenting its facilities and organizing stretcher and first-aid teams. In small systems or facilities, health teams should be set up under the supervision of private or public health agencies. As a minimum, first-aid personnel and equipment should be provided in all facilities.

The duties of a facility health director include:

(1) Making an appraisal of the medical personnel, equipment, supplies, and other health resources of the facility and determining their adequacy for coping with large-scale disaster.

(2) Augmenting the health services staff, if necessary.

(3) Providing sufficient first-aid equipment for first-aid units stationed within the facility and

stockpiling consumable surgical supplies as recommended by the local civil defense organization.

(4) Organizing classes in first-aid and supervising first-aid stations.

(5) Recruiting and training personnel for emergency duties.

(6) Providing for identification and transportation of casualties.

(7) Providing advice and supervision to the engineering services on environmental health hazards, such as contaminated water supplies and excessive concentrations of toxic chemicals in the air.

(8) In large facilities, training and organizing radiological monitoring units.

(9) Participating in community planning for emergency mortuary service in case of disaster.

(10) Integrating plans with nearby plants and nearby institutions and with local civil defense organization to pool emergency medical equipment and supplies and to share trained personnel.

(11) Studying the industrial hazards involved in operations within the facility and making plans to cope with health emergencies that might arise if protective devices fail.

(12) Attending courses to train himself and his staff in the medical aspects of special weapons defense.

(13) Arranging for decontamination of people who have been exposed to atomic, biological, or chemical warfare agents.

It is unlikely that any system or facility, even large ones, could alone take care of the huge number of casualties that might result from modern war. Each would have to draw on the resources of neighboring plants and on the community for help.

In addition, if each facility were to attempt to stockpile bandages, dressings, anaesthetics, drugs, ambulances and other health supplies on a scale keyed to modern warfare it would lean to uneconomical overlap and would cause excessive drain on facility budgets and on critical supplies of the nation. Therefore, plans should be made with neighboring facilities, health agencies, and local civil defense groups to pool resources and share health personnel in event of disaster. To derive greatest benefit from joint planning, all equipment and supplies should be standardized and joint text exercises should be held.

f. *Guard Services*

The facility guard services are a vital part of the emergency program and are responsible for maintaining order and discipline, for safeguarding people and property and for directing traffic. They also support other services in carrying out their duties.

When disaster strikes, the initial problem facing guards is traffic control and panic prevention. In an emergency, traffic can get out of hand, resulting in panic and the break-down of protective operation. Entrances, traffic lanes, and roads must remain clear for free passage of fire equipment, ambulances, rescue trucks and other emergency vehicles. Guards also must control mass action to prevent panic and assist other services in utilizing the help of all able-bodied individuals.

The facility guard chief is responsible for drawing up traffic plans to evacuate the facility or to obtain assistance from outside. He should make plans for the safeguarding of vital records, specifications and materials and for the protection of vital equipment. The responsibility of guarding against entry of unauthorized persons is accentuated in the emergency because subversive agents may rely on the ensuing confusion to gain entrance to restricted areas of the system or facility. The inclusion of plans for auxiliary guards in the protection program is essential.

The guard chief is also responsible for determining the immediate protective measures which should be instituted when unexploded ordnance is found. He should instruct his men in methods of roping off areas around unexploded ordnance. Combustible materials should be removed from the immediate vicinity where feasible, and the control room notified at once. The local civil defense authorities should be notified and they in turn will notify the Army, which has responsibility in matters of unexploded ordnance.

The guard services should be mobile and ready to support all other protective services. They should be familiar with the layout of the plant, including fire-alarm boxes, first-aid stations, communications with the control center, power switches and with traffic routes in and leading to the facility.

All questionable situations should be reported immediately to the control room. If this habit is developed in the course of simulated tests, it will tend to insure prompt reporting in an emergency.

Liaison should be established with the local police and civil defense and joint traffic procedures worked out to avoid conflict of plans in an emergency. Liaison with these two groups is also important in obtaining assistance, if needed, in the emergency.

g. *Warden Services*

The warden service, functioning under the direction of the security director, is concerned with the safeguarding of life and property. This includes informing personnel of civil defense regulations, such as warning and shelter regulations, training personnel in self-protection measures, di-

recting people to shelter areas, preventing panic and performing first-aid and elementary rescue. Wardens will also assist other services, such as fire, police, etc., as the occasion demands. Wardens, because of their close contact with personnel of a facility are in a good position to see that every able-bodied individual is given a job in the emergency.

A warden chief should be appointed to organize and train the warden service. He should divide the facility into zones and assign a warden to each zone. The size of the zone or number of people in it will vary with each facility, but the warden should exercise reasonable control over the zone and the people in it.

The warden duties can be broken down into three phases, namely, pre-attack, alert and post-attack:

(1) PRE-ATTACK

(a) Informing all personnel of civil defense regulations.

(b) Training all personnel in basic self-protection (many standard texts on this subject are included in the bibliography).

(c) Maintaining a record of home address, nearest kin, physical handicap and similar information about personnel.

(d) Designating personnel in their area to secure classified information or other special items in the event of emergency.

(e) Cooperating with all services in the elimination of hazards by keeping all areas clear of trash, keeping passageways clear, etc.

(2) ALERT

(a) Directing personnel to shelter areas.

(b) Preventing panic.

(c) Keeping all passageways, roads, etc., clear.

(d) Getting first-aid equipment ready.

(3) POST-ATTACK

(a) Reporting conditions in their area to the security director.

(b) Rendering first-aid.

(c) Performing elementary rescue.

(d) Extinguishing fires within their capabilities.

(e) Requesting whatever help is needed.

(f) Assisting other services as necessary.

(g) Accounting for all personnel in their area.

h. *Engineering Services*

The engineering services have the responsibility of clearing rubble and debris, demolition, shoring and repairing buildings, restoring damaged utilities and roads, decontaminating areas and buildings, and assisting in the rescue of trapped persons. The engineering services should consist of maintenance and repair units, demolition and clearance units, decontamination units and rescue units.

Maintenance and repair units should be organized in different areas of the facility to restore utilities, to make emergency repairs to buildings and to restore communications.

Demolition and clearance units should reinforce or tear down damaged walls, structural framework, and unsound foundations, and remove debris immediately after an attack. Dealing quickly with these problems prevents more personnel from becoming casualties and clears the way for other protective services to operate.

Decontamination units should be formed as needed to make structures, equipment, and frequented areas inside and outside the facility safe from poisonous gases or radioactive materials. These units also should disinfect water mains after repair to insure potable water.

Rescue units should be formed to free persons trapped in wreckage. Men who know the construction features of the plant should be selected for this work.

The engineering chief also should maintain liaison with his counterparts in the community and neighboring plants for possible pooling of equipment and supplies in an emergency and with the local civil defense authorities.

i. *Welfare Services*

Immediately after any disaster, many persons will need welfare assistance. This will include emergency feeding and housing, financial aid and assistance in locating families. Where the size of the organization justifies, the members of these services should be organized into subordinate groups to perform the above functions.

Probably more than in any other sphere, liaison with civil defense is needed with respect to welfare services because it is essentially a community problem. The facility security director should consult the local civil defense authorities and make plans to cooperate with them in welfare matters. Local social agencies can also give valuable assistance in this work.

2. RESTORATION OF PRODUCTION OR SERVICE

In a large scale attack it must be anticipated that there will be concentrated destruction and damage to systems, facilities, processes, and equipment far in excess of the damage commonly caused by forces of nature. In this event, the problem of restoring service will be complicated by such conditions as panic, impassable streets, extensive fires, etc.

a. *Planning*

It is essential that plans be developed to cover possible conditions which may occur in the event of a major attack.

The difference between an emergency and a disaster is largely one of degree. Adequate disaster planning will cover both conditions, varying only in the extent of application.

The normal operating organization should be adapted to provide for contingencies arising from emergency and disaster conditions, and for the probability of casualties, involuntary absences, and the magnitude of the physical restoration problems. All key functions should be covered by designating alternates and the line of succession of authority.

Operating organizations are keyed to function with a complete system of communication and transportation. The extension of plans covering operations during disaster must recognize the probable failure of such facilities and make provision for alternate means of communication and transportation. Provision should be made for the transfer of executive and administrative staff headquarters to alternate locations in recognition of the possibility of destruction of normal facilities. Such alternate headquarters should be carefully selected after due consideration of such factors as communication, transportation, normal distribution of personnel both during and after business hours, availability of food and water and sanitation facilities. The relative probability of destruction by enemy action and the risk of access routes being jammed by refugees are also pertinent.

Advance consideration should be given to liaison with and enlisting the aid of selected agencies that may best contribute to rapid production or service restoration. Active coordination with the military and Civil Defense groups should be planned.

(1) PERSONNEL

The extraordinary nature and extent of possible damage may require the assignment of non-operating personnel to operating duties. It is essential that the entire personnel roster be studied and assignments made to such duties in advance as may be practicable.

(2) TRAINING

All employees should be trained in the specific channels indicated by the unusual nature of the problems that may be expected from specific enemy actions heretofore indicated as possible. In addition, training should be introduced covering the duties that are assigned to employees outside of their normal job specifications.

(3) EQUIPMENT, TOOLS AND MATERIALS

Equipment, tools and materials should be protected as far as practicable by dispersion. Additional sources of supply by purchase, loan or contract should be established in advance. Coordination with other petroleum or gas organizations, and allied supply and construction industries should be planned, and key personnel to effect this coordination should be assigned in advance.

(4) RECORDS

Decentralization or duplication of essential records should be thoroughly studied and provision made to assure the availability of such records when required.

(5) AUXILIARY SUPPORTING SERVICES

Recognition should be given to the requirement of auxiliary services to support the operating forces under emergency conditions. For instance, it may be necessary to provide food, quarters, and medical aid to individuals on duty under disaster conditions for extended periods of time. Also, such services as building maintenance, plumbing, electrical maintenance and communication, messengers, transportation, fuel supply and policy protection, which usually are furnished by outside agencies, may have to be provided by the organization. The assurance that provision has been made for aiding employees' families may help materially in keeping personnel on the job.

b. *Testing the Plan*

The geographic distribution of facilities and the nature of the petroleum and gas industries makes it impractical to prepare detail plans for every conceivable situation. However, the selection of a few critical cases of assumed damage and their theoretical solution is recommended to test the organization's ability to cope with possible damage and indicate the magnitude of the restoration problem.

The organization should be prepared to shift from centrally controlled operations to local control in limited areas with a maximum of authority and autonomy vested in the local area supervision.

c. *Selective Restoration*

All plans should be predicated on the necessity of restoring production and service selectively, giving precedence to vital elements in the national defense and civilian economy. All employees exercising control functions should be thoroughly indoctrinated in this principle. The following services are among those that require the highest priority.

Hospitals, including improvised hospitals.
Water supply.
Sanitation Service.

Cold Storage.
Transportation.
Warehouses and docks.
Food Processing.
Municipal and Government Agencies.
Military and Naval Installations.
Communications.
Civil Defense Mass Care Centers.
Fuel Supply.
Essential Industries.

The relative order of priority must be a matter of judgment in each individual case and under some circumstances will be dictated by military necessity.

The following is a check list of items which a disaster plan should cover:

(1) Alternate locations for important headquarters dispatching and message centers.

(2) Alternate means of transportation and communication, including self-contained units and messengers.

(3) Dispersal of critical items required for emergency repairs, including vehicles, tools and equipment. Provide, to appropriate people, a catalog of available material and its location.

(4) List of key individuals in adjoining facilities and Government Agencies and how they can be reached.

(5) Interchange of repair crews, material and equipment with other petroleum and gas systems or facilities.

(6) Interconnection of water, steam and electric systems with neighboring plants, wherever possible, and when feasible, alternate power supply.

(7) Instructions and priority for essential load restorations and production facility restoration.

(8) If practicable, provide helicopter or small plane for assessment of damage and observation.

(9) Emergency medical care, feeding, transportation and quartering of restoration crews.

(10) Organize radiological teams, damage survey and debris clearance crews.

(11) Maintain close liaison with Civil Defense.

(12) Provide for the transmission of appropriate vital information and advice to the public.

(13) Establishing cash credits in decentralized locations.

(14) Personnel, records, training, additional sources of supply, etc.

(15) Mobilization procedure to put plan in action.

BIBLIOGRAPHY

The inclusion of the pamphlets listed in the Bibliography does not constitute an endorsement by the Facilities Protection Board.

The following publications may be obtained from the Superintendent of Documents, United States Government Printing Office, Washington 25, D. C., at the cost indicated:

1. Air Raid Alert Card, Federal Civil Defense Administration, 1951. Price 5 cents.

2. Civil Defense Against Atomic Warfare, a selected reading list. A list of official reports of the U. S. Atomic Energy Commission and other Government Agencies, together with significant book and periodical publications. Prepared for the National Security Resources Board by the U. S. Atomic Energy Commission, March 1950. Price 10 cents.

3. Civil Defense in Industry and Institutions, Reprinted from Federal Civil Defense Administration, Publication AC-16-1. Price 25 cents.

4. Damage from Atomic Explosion and Design of Protective Structures, Prepared for the National Security Resources Board by the Department of Defense and U. S. Atomic Energy Commission. Price 10 cents.

5. The Effects of Atomic Weapons—Prepared under the direction of the Los Alamos Scientific Laboratory, Los Alamos, New Mexico, June 1950. Price $1.25. (Paper bound).

6. Emergency Action to Save Lives—Prepared by the Federal Civil Defense Administration, 1951. Price 5 cents.

7. Emergency Defense Activities Handbook. General Services Administration. April-September 1952. Price 30 cents.

8. "Engineering Services," AG-13-1, Federal Civil Defense Administration. Price 15 cents.

9. Federal Register, Vol. 16, Number 167, of August 28, 1951, (Page 8677) containing Coast Guard rules and regulations, pertaining to Security of Waterfront Facilities, 33 CFR, Part 126.

10. Federal Register, Vol. 16, Number 217 of November 7, 1951, (Page 11311) interpreting part 126.15 of Coast Guard CFR 33, Part 126 (see No. 9 above).

11. Finger Print Card—U. S. Government Form No. 16-63416-1. Price $1.50 per hundred.

12. Fire Services—Prepared by the Federal Civil Defense Administration, 1951. Price 15 cents.

13. The Geiger-Muller Counter, issued Jan. 23, 1950 by the U. S. Department of Commerce, National Bureau of Standards, Circular 490. Price 20 cents.

14. Health Services and Special Weapons Defense—U. S. Civil Defense—prepared by Federal Civil Defense Administration—Publication AG-11-1. Price 60 cents.

15. How to Be Cleared for Handling Classified Military Information Within Industry—Prepared by the Munitions Board, Department of Defense. Price 10 cents.

16. Industrial Security Manual for Safeguarding Classified Matter—Prepared by the Munitions Board, Department of Defense. Price 10 cents. 13 December 1951.

17. Is Your Plant a Target—Industrial Dispersion—Prepared by the National Security Resources Board, August 1951. Price 25 cents.

17a. Questions and Answers on the Industrial Dispersion Program, National Security Resources Board, Superintendent of Documents. Gratis Supplement to "Is Your Plant a Target?".

18. Medical Aspects of Atomic Weapons—Prepared by the Federal Civil Defense Administration, 1951. Price 10 cents.

19. Outdoor Warning Device Systems—Prepared by the Federal Civil Defense Administration, 1951. Price 15 cents.

20. Police Services—Prepared by the Federal Civil Defense Administration—Publication AG-10-1, May 1951. Price 20 cents.

21. Principles of Civil Defense Operations—Prepared by the Federal Civil Defense Administration, 1951. Price 20 cents.

22. Principles of Plant Protection—Prepared by Industrial Security Division, Office of Manpower, Munitions Board, August 1, 1950. Price 15 cents.

23. The Rescue Service—Federal Civil Defense Administration—Publication AG-10-1, May 1951. Price 20 cents.

24. "The Story of Defense Mobilization"—Executive Office of the President, Office of Defense Mobilization—GPO, 1952, Form No. 0-984507. Gratis.

25. Survival Under Atomic Attack—Prepared by the Civil Defense Office, National Security Resources Board, Document #130. Price 10 cents.

26. This is Civil Defense—Federal Civil Defense Administration, 1951. Price 10 cents.

27. United States Civil Defense—Prepared by the National Security Resources Board, Document #128, September, 1950. Price 25 cents.

28. United States Government Organization Manual, 1951-52, General Services Administration. Revised July 1951. Price $1.00.

29. The Warden Service—Federal Civil Defense Administration, 1951. Price 20 cents.

29a. Question and Answer Guide on the National Industrial Dispersion Program—National Security Resources Board, Feb. 1952.

30. Water Supplies for Wartime Fire Fighting—Federal Civil Defense Administration—Publication TM-9-1, July 1951. Price 10 cents.

31. What If War Hits Our Homes—Published by the Armed Forces Information and Education Division, 1951. Price 5 cents.

32. What You Should Know About Biological Warfare—Prepared by the Federal Civil Defense Administration, 1951. Price 10 cents.

33. Executive Order 10290, 24 September 1951—"Prescribing Regulations Establishing Minimum Standards for the Classification, Transmission, and Handling, by Departments and Agencies of the Executive Branch, of Official Information which Requires Safeguarding in the Interest of the Security of the United States."

Other Publications and sources are listed below:

34. Air Raid Precautions for Industrial and Business Premises—Ministry of Pensions and National Health, Ottawa, Canada, 1942.

35. Air Raid Precautions for Personnel, Plants and Buildings—Metropolitan Life Insurance Company, 1950.

36. Air Raid Shelters for Persons Working in Factories, Mines and Commercial Buildings—Memorandum on the Revised Code. His Majesty's Stationery Office, London.

37. Atomic Bombing—A Problem for Civil Defense. By Lt. Col. C. F. Hawkins, Headquarters, First Army, New York, New York, 1949.

38. Atomic Warfare, Manual of Basic Training, Vol. II. His Majesty's Stationery Office, London, 1950.

39. Bank Personnel and Records Protection Guide—Bank Management Publication 124, Bank Management Commission, American Bankers Association, 1951.

40. Bombproofing for Business—U. S. News and World Report, August 25, 1950.

41. The Care of Records in a National Emergency—Publication No. 18—Bulletin of the National Archives, No. 3, December 1941.

42. Civil Defense Industrial Plant Protection—Proposed by the Civil Defense Department, National Health and Welfare, Ottawa, Canada, 1951.

43. Civil Defense Program Applicable to Gas Utilities and Supplying Companies—comprising a basic plan adopted by New York Public Service Commission; available through the Edison Electric Institute; dated August 30, 1950.

44. Civil Defense Supplement to the American Red Cross First Aid Textbook—American Red Cross, 1951.

45. Controlling Industrial Fire Hazards—the National Board of Fire Underwriters, New York, 1948.

46. Danger—Enemies from Within—Reprinted from Commerce Magazine—Chicago Association of Commerce, 1 N. LaSalle Street, Chicago 2, Illinois. Price 35 cents.

47. Disaster Control—Reader Service Department, American Machinist, 330 W. 42nd Street, New York 18, New York.

48. The Effects of Structures and Personnel—Canadian Civil Defense, Manual No. 2.

49. The Effects of the Atomic Bombs at Hiroshima and Nagasaki—Report of the British Mission to Japan—Published by His Majesty's Stationery Office, London, 1946. 1 shilling net.

50. Emergency Communications for Plant Protection—issued by Motorola, Inc., as a supplement to Chapter V, Section 3b., of the Munitions Board's "Principles of Plant Protection."

51. Employee Organization for Fire Safety—National Fire Protection Association, Boston, Massachusetts, 1945.

52. Executive Planning—If An A-Bomb Falls—Studies in Personnel Policy #108, Prepared by National Industrial Conference Board, Inc., 247 Park Avenue, New York 17, New York—September 1950.

53. Explosions, Their Anatomy and Destructiveness. By C. S. Robinson, McGraw-Hill Book Company, 1944.

54. Fire and The Air War, National Fire Protection Association, Boston, 1946.

55. Fire Defense, National Fire Protection Association.

56. Fire Protection, Air Raid Precautions Handbook No. 13. His Majesty's Stationery Office. London.

57. Flood Damage—How to Limit and Repair It, by Gene Fuller, John King and Jim O'Connor. Power, 330 West 42nd Street, New York.

58. How to Take Finger Prints, Obtainable from the Identification Division, Federal Bureau of Investigation, Washington 25, D. C. Gratis.

59. Handbook of Fire Protection—Crosby-Fiske Forester.

60. Highlights of the U. S. Civil Defense Plan—Release #175 of National Security Resources Board, September 18, 1950. Available through Edison Electric Institute.

61. Home Air Raid Shelters—Technical Pamphlet #2—Structural Protection Committee, Massachusetts Civil Defense Agency, June 1, 1951.

62. How to Survive an Atomic Bomb, by Richard Gerstell, Ph.D. Bantam Books, Inc., 1107 Broadway, New York, N. Y. Price 25 cents.

63. Industrial Guard's Manual. By Harry D. Farren. National Foremen's Institute, Inc., New York. 1943.

64. Internal Security Laws—Prepared by the Legislative Reference Service, Library of Congress, Washington 25, D. C.

65. Mobilizing for Atomic War—Studies in Business Policy, No. 46, prepared by the National Industrial Conference Board, Inc., July 1950. Price $1.50.

66. Organization Chart and Sub-Committee of the Disaster Preparedness and Relief Committee, Boston Metropolitan Chapter, American National Red Cross, October 23, 1950.

67. Organization for Civil Defense—Canadian Civil Defense Manual #1, Ottawa, Ontario.

68. Organizing Your Plant for Fire Safety. Ass'd Factory Mutual Fire Insurance Co. 's., Boston, 1950.

69. Patterns of Panic. By J. A. M. Meerloo, M.D., International Universities Press. 1950.

70. Plans and Procedures to Meet a National Emergency in Columbia Gas System Companies—Received with American Gas Association Information Service of November 1, 1950.

71. Plant Protection—A-Bomb is the Problem. Business Week Magazine, March 21, 1951. McGraw-Hill Publishing Company, 330 West 42nd Street, New York 18, New York.

72. Plant Protection for National Defense, Detex Watchclock Corp., New York, New York.

73. Plant Protection Guide for Chicago Civil Defense Committee. Distributed by the Chicago Association of Commerce and Industry. 1 North LaSalle Street, Chicago, Illinois.

74. Primer for Plant Protection. Department of Manufacture, Chamber of Commerce of the United States, Washington, D. C.

75. Principles of Plant Protection—Military and Civil Defense Commission for Pennsylvania, Harrisburg, Pa.

76. The Problem of Reducing Vulnerability to Atomic Bombs. By Ansley J. Coal, Princeton University Press, 1947.

77. Protection of Electric Service from Sabotage and Enemy Action—Published by Edison Electric Institute, December 1950 (publication No. 50-14). Price 20 cents.

78. Protection from the Atomic Bomb—Prepared for the Civil Defense Agency of the Commonwealth of Massachusetts by John W. M. Bunker, Dean of the Graduate School, M. I. T., and others. November 1950.

79. Public Utilites and Civil Defense—An article by the Honorable Benjamin F. Feinberg, Chairman, New York Public Service Commission, appearing in the November 23, 1950 issue of the Public Utilities Fortnightly.

80. Radiation Hazards in the Event of an Atomic Disaster—A manuscript currently in use in the Red Cross Instructors' Course.

81. Reaction of Buildings to the Atomic Bomb—Technical Pamphlet #3—Structural Protection Committee, Massachusetts Civil Defense Agency, June 1, 1951.

82. Recommendations for Increasing the Blast Resistance of Proposed or Existing Buildings—Technical Pamphlet #1—Structural Protection Committee, Massachusetts Civil Defense Agency, June 1, 1951.

83. Recommendations on Air Raid Shelter Program. By Dr. Merit P. White, of the Structural Protection Committee, Massachusetts Civil Defense Agency—CDA 317. February 6, 1951.

84. Report on Philadelphia Gas Works Co. Defense Planning Program by Charles G. Simpson, Assistant Engineer of Production, at A. G. A. Safety Conference, Washington, September 19, 1950—from notes taken by F. G. Harriman.

85. The article, "Restoration of Gas Service with Safety After a Major Interruption," contained in Current Safety Topics in the PUBLIC UTILITIES INDUSTRIES, Volume 25, Transactions, 39th National Safety Congress—National Safety Council, 425 North Michigan Avenue, Chicago 11, Illinois.

86. Sabotage—How to Guard Against It—Reprint; published by National Foreman's Institute, Inc., 1950.

87. Safeguarding Industry. National Board of Fire Underwriters, New York, New York, 1947.

88. Safeguarding Records from Air Raids—Policyholders Service Bureau, Metropolitan Life Insurance Co. A 1942 report reprinted in 1950.

89. Salvaging Operations. National Fire Protection Association, Boston, Massachusetts, 1944.

90. Some Aspects of Radiological Defense. By William H. Sullivan, Scientific Director, Naval Radiological Defense Laboratory, San Francisco Naval Shipyard, San Francisco 24, California, July 24, 1950.

91. Some Public Health Aspects of An Atomic Explosion, by William H. Sullivan, Scientific Director, Naval Radiological Defense Laboratory, San Francisco Naval Shipyard, San Francisco 24, California, June 3, 1950.

92. Special isue on "Civil Defense Against Atomic Attack" of the Bulletin of the Atomic Scientists for Aug.-Sept. 1950. Price $1.00.

93. Structural Defense. Air Raid Precautions Handbook No. 5. His Majesty's Stationery Office, London.

94. The Training Supervisor's Responsibility in the Light of Approaching Problems of Civil Defense—A 17-page outline currently in use by the American National Red Cross in training their instructors.

95. Training Manual for Auxiliary Firemen—National Fire Protection Association.

96. You Can Survive Tomorrow's Atomic Attack—Prepared by Mort Weisinger and based upon official recommendations set forth by the Atomic Energy Commission and the Department of National Defense. Published by the P. & G. Publishing Company, 480 Lexington Avenue, New York, N. Y. Price 25 cents.

97. "War Protection of the Gas Industry," March 1942, American Gas Association, 420 Lexington Avenue, New York, New York.

98. We Are Not Helpless—How we can defend ourselves against atomic weapons. A series of non-technical articles reprinted from The New York Times. Price 10 cents.

99. What About Safeguards Against Industrial Sabotage? A Survey Report—Mill & Factory Magazine for April 1951. Conover-West Publications, Inc., 205 East 42nd Street, New York 17, New York.

100. Standard for Central Station Burglar Alarm Systems, Underwriters' Laboratories, Inc., Chicago, Illinois.

101. Standard for Local Burglar Alarm Systems, Underwriters' Laboratories, Inc., Chicago, Illinois.

102. Standard for Installation, Classification and Certification of Burglar Alarm Systems, Underwriters' Laboratories, Inc., Chicago, Illinois.

A few of the motion pictures available through local Civil Defense or Film distributors are:

1. Target U.S.A.—Prepared by the Research Institute of America.

2. Survival Under Atomic Attack—Prepared by Federal Civil Defense Administration.

3. Our Cities Must Fight—Prepared by Federal Civil Defense Administration

4. What You Should Know About Biological Warfare—Prepared by Federal Civil Defense Administration.

APPENDIX "A"

PERSONNEL SECURITY QUESTIONNAIRES

INSTRUCTIONS.—All sections must be completed. Write "None" when applicable. Type or print all answers. If space not adequate for complete answers, attach a supplemental sheet to this form. All addresses must show street number, street, city, and State.

1. NAME (Last, first, middle)

2. OTHER NAMES (Include maiden name, if married woman)

3. PRESENT ADDRESS DATE

4.. ALL OTHER ADDRESSES FOR PAST 10 YEARS DATE

5. DESCRIPTION: (check which) ☐ MALE ☐ FEMALE

RACE	HEIGHT	WEIGHT	COLOR EYES	COLOR HAIR

6. (Check which)
☐ SINGLE ☐ DIVORCED
☐MARRIED ☐ WIDOW (ER)

7. BIRTH DATE

DAY	MONTH	YEAR

8. BIRTHPLACE (City, county, State, and country)

9. CITIZENSHIP: U.S. ☐ ALIEN ☐

IF U.S. CITIZEN, INDICATE WHETHER:

(A) BY BIRTH ☐

(B) DERIVATIVE ☐

DATE

CERTIFICATE NO.

PLACE

(C) BY NATURALIZATION ☐

PETITION NO.

DATE

CERTIFICATE NO.

PLACE

IF ALIEN INDICATE ALIEN REGISTRATION NO.

DATE

PORT OF ENTRY

10. DRAFT BOARD NUMBER AND ADDRESS WITH WHICH REGISTERED

11. SOCIAL SECURITY NO.

12. MILITARY SERVICE

SERIAL NO.	BRANCH	FROM (Yr.)	TO (Yr.)

13. EDUCATION (All schools above high school)

NAME OF SCHOOL	ADDRESS	FROM (Yr.)	TO (Yr.)	DEGREES

APPENDIX "A" (cont'd)

14. FOREIGN COUNTRIES VISITED (Since 1930) (Exclusive of military service)

COUNTRY	DATE LEFT U.S.A.	DATE RETURNED U.S.A.	PURPOSE

15. EMPLOYMENT FOR LAST 10 YEARS (LIST ALL EMPLOYMENT DATES INCLUDING PRESENT EMPLOYMENT AND ALL DATES OF UNEMPLOYMENT.) GIVE NAME UNDER WHICH EMPLOYED IF DIFFERENT FROM NAME NOW USED.

DATE FROM-TO	NAME OF EMPLOYER (COMPANY OR ORGANIZATION)	TYPE OF WORK	ADDRESS (Where employed)	REASON FOR LEAVING

(Indicate by * after name of employer, all investigations and clearances received during past two years)

16. ARE YOU NOW, OR HAVE YOU EVER BEEN A MEMBER OF ANY ORGANIZATION, ASSOCIATION, MOVEMENT, GROUP, OR COMBINATION OF PERSONS WHICH ADVOCATES THE OVERTHROW OF THE CONSTITUTIONAL FORM OF GOVERNMENT OF THE UNITED STATES, OR OF ANY ORGANIZATION, ASSOCIATION, MOVEMENT, GROUP, OF COMBINATION OF PERSONS WHICH HAS ADOPTED A POLICY OF ADVOCATING OR APPROVING THE COMMISSION OF ACTS OF FORCE OR VIOLENCE TO DENY OTHER PERSONS THEIR RIGHTS UNDER THE CONSTITUTION OF THE UNITED STATES OR OF SEEKING TO ALTER THE FORM OF GOVERNMENT OF THE UNITED STATES BY

UNCONSTITUTIONAL MEANS?..... Answer "Yes" or "No"

(See Attorney Generals list of subversive organizations attached.)

17. IF YOUR ANSWER TO QUESTION 16 IS "YES," STATE THE NAME OF THE ORGANIZATION, DATES OF MEMBERSHIP, AND EXTENT OF PARTICIPATION. AN EXPLANATION REGARDING MEMBERSHIP IN ANY OF THESE ORGANIZATIONS MAY BE ATTACHED HERETO ON A SEPARATE SHEET OF PAPER, IF YOU DESIRE TO EXPLAIN THE CIRCUMSTANCES OF YOUR MEMBERSHIP.

NAME	ADDRESS	FROM	TO	OFFICE HELD

18. RELATIVES (Parents, spouse, divorced spouse, children, brothers, and sisters, living or dead)

RELATION	NAME IN FULL	AGE	ADDRESS	COUNTRY OF BIRTH	PRESENT CITIZENSHIP

19. REFERENCES (Name three persons, not relatives or employers, who are well acquainted with you)

NAME	ADDRESS	YEARS KNOWN

20. HAVE YOU EVER BEEN ARRESTED, INDICTED, OR SUMMONED INTO COURT AS A DEFENDANT IN A CRIMINAL PROCEEDING, OR CONVICTED, FINED OR IMPRISONED OR PLACED ON PROBATION IN CONNECTION WITH SUCH A PROCEEDING, OR HAVE YOU BEEN ARRESTED OR REQUIRED TO DEPOSIT BAIL OR COLLATERAL FOR

THE VIOLATION OF ANY LAW, POLICE REGULATION OR ORDINANCE (EXCLUDING MINOR TRAFFIC VIOLATIONS)?..... _____

Answer "Yes" or "No"

IF YOUR ANSWER IS "YES," LIST ALL SUCH CASES IN 21. IN EACH CASE GIVE: (1) THE CHARGE OR NATURE OF THE OFFENSE; (2) THE DATE; (3) THE PLACE WHERE ARRESTED; (4) DISPOSITION OR THE PENALTY IMPOSED, IF ANY.

21. ARRESTS (Include all arrests and fines other than minor traffic violations)

CHARGE	DATE	PLACE WHERE ARRESTED	DISPOSITION

CERTIFICATION

I CERTIFY THAT THE ABOVE INFORMATION IS CORRECT AND COMPLETE TO THE BEST OF MY KNOWLEDGE AND BELIEF. I MAKE THIS STATEMENT WITH THE UNDERSTANDING THAT ANY FALSE STATEMENT OR OMISSION OF MATERIAL FACT MAY BE SUFFICIENT CAUSE FOR REJECTION OF MY APPLICATION OR DISMISSAL AFTER EMPLOYMENT.

(DATE)	(USUAL SIGNATURE OF PERSON FILLING OUT QUESTIONNAIRE) (Sign original only)

TO BE FILLED OUT BY A RESPONSIBLE MANAGEMENT OFFICIAL

NAME OF INDIVIDUAL	ADDRESS
BRIEF DESCRIPTION OF DUTIES (Description should not reveal vital information)	WILL PERSON HAVE ACCESS TO A RESTRICTED AREA OR VITAL INFORMATION? YES NO
	FINGERPRINT CARD ATTACHED
	REFERRED FOR INVESTIGATION
FORMER INVESTIGATIONS AND CLEARINGS VERIFIED	CLEARANCE GRANTED

APPENDIX "A" (cont'd)

Set forth below is a list of the organizations designated by letters of November 24, 1947, May 27, 1948, April 21, 1949, July 20, 1949, September 26, 1949, August 24, 1950, September 5, 1950, January 25, 1951, April 18, 1951, April 25, 1951, and August 31, 1951, by the Attorney General in accordance with the provisions of Executive Order No. 9835, as Totalitarian, Fascist, Communist, or Subversive, or which have adopted a policy of advocating or approving the commission of acts of force and violence to deny others their rights under the Constitution of the United States, or which seek to alter the form of the Government of the United States by unconstitutional means.

Totalitarian:

Black Dragon Society
Central Japanese Association (Beikoku Chuo Nipponjin Kai)
Central Japanese Association of Southern California
Dai Nippon Butoku Kai (Military Virtue Society of Japan or Military Art Society of Japan)
Heimuska Kai, also known as Nokubei Heieki Gimusha Kai, Zaibel Nihonjin, Heijaku Gimusha Kai, and Zaibei Heimusha Kai (Japanese Residing in America Military Conscripts Association)
Hinode Kai (Imperial Japanese Reservists)
Hinomaru Kai (Rising Sun Flag Society—a group of Japanese War Veterans)
Hokubei Zaigo Shoke Dan (North American Reserve Officers Association)
Japanese Association of America
Japanese Overseas Central Society (Kaigai Dobo Chuo Kai)
Japanese Overseas Convention, Tokyo, Japan, 1940
Japanese Protective Association (Recruiting Organization)
Jikyoku Iinkai (The Committee for the Crisis)
Kibei Seinen Kai (Association of U. S. Citizens of Japanese Ancestry who have returned to America after study in Japan)
Nanka Teikoku Gunyudan (Imperial Military Friends Group or Southern California War Veterans)
Nichibei Kogyo Kaisha (The Great Fujii Theatre)
Northwest Japanese Association
Peace Movement of Ethiopia
Sakura Kai (Patriotic Society, or Cherry Association—composed of veterans of Russo-Japanese War)
Shinto Temples
Sokoku Kai (Fatherland Society)
Suiko Sha (Reserve Officers Association of Los Angeles)

Fascist:

American Nationalist Party
American National Labor Party
American National Socialist League
American National Socialist Party
American Patriots, Inc.
Ausland-Organization der NSDAP, Overseas Branch of Nazi Party
Association of German Nationals (Reichsdeutsche Vereinigung)
Central Organization of the German-American National Alliance (Deutsche-Amerikanische Einheitsfront)
Citizens Protective League
Committee for Nationalist Action
Dante Alighieri Society (between 1935 and 1940)
Federation of Italian War Veterans in the U. S. A., Inc. (Associazione Nazionale Combattenti Italiani, Federazione degli Stati Uniti d'America)
Friends of the New Germany (Freunde des Neuen Deutschlands)
German-American Bund (Amerikadeutscher Volksbund)
German-American Republican League
German-American Vocational League (Deutsche-Amerikanische Berufsgemeinschaft)
Kyffhaeuser, also known as Kyffhaeuser League (Kyffhaeuser Bund) Kyffhaeuser Fellowship (Kyffhaeuser Kameradschaft)
Kyffhaeuser War Relief (Kyffhaeuser Kreigshilfswerk)
Lictor Society (Italian Black Shirts)
Mario Morgantini Circle
National Blue Star Mothers of America (not to be confused with the Blue Star Mothers of America organized in February 1942)
Nationalist Action League

Communist:

Abraham Lincoln Brigade
Abraham Lincoln School, Chicago, Ill.
Action Committee to Free Spain Now
Alabama Peoples Educational Association
American Association for Reconstruction in Yugoslavia, Inc.
American Branch of the Federation of Greek Maritime Unions
American Committee for European Workers' Relief
American Committee for Protection of Foreign Born
American Committee for Spanish Freedom
American Committee for Yugoslav Relief, Inc.
American Council for a Democratic Greece, formerly known as the Greek American Council; Greek American Committee for National Unity
American Council on Soviet Relations
American Croatian Congress
American Jewish Labor Council
American League Against War and Fascism
American League for Peace and Democracy
American Peace Mobilization
American Polish Labor Council
American Rescue Ship Mission (a project of the United American Spanish Aid Committee)
American-Russian Fraternal Society
American Russian Institute, New York
American Russian Institute, Philadelphia
American Russian Institute (of San Francisco)
American Russian Institute of Southern California, Los Angeles
American Slav Congress
American Youth Congress

Communists—Continued:

American Youth for Democracy
Armenian Progressive League of America
Boston School for Marxist Studies, Boston, Mass.
California Labor School, Inc., 216 Market Street, San Francisco, Calif.
Carpatho-Russian Peoples Society
Central Council of American Women of Croatian Descent, also known as Central Council of American Croatian Women, National Council of Croatian Women
Cervantes Fraternal Society
Citizens Committee to Free Earl Browder
Citizens Committee for Harry Bridges
Citizens Committee of the Upper West Side (New York City)
Civil Rights Congress and its affiliated organizations
Civil Rights Congress for Texas
Civil Rights Congress, Milwaukee Chapter
Civil Rights Congress of Michigan
Comite Coordinador Pro Republica Espanola
Committee for a Democratic Far Eastern Policy
Committee to Aid the Fighting South
Commonwealth College, Mena, Ark.
Communist Party, U. S. A., it subdivisions, subsidiaries, and affiliates
Communist Political Association, its subdivisions, subsidiaries, and affiliates
Connecticut State Youth Conference
Congress of American Revolutionary Writers
Congress of American Women
Council on African Affairs
Council for Pan-American Democracy
Croatian Benevolent Fraternity
Daily Worker Press Club
Dennis Defense Committee
Detroit Youth Assembly
Emergency Conference to Save Spanish Refugees (founding body of the North American Spanish Aid Committee)
Finnish-American Mutual Aid Society
Florida Press and Educational League
Friends of the Soviet Union
Garibaldi American Fraternal Society
George Washington Carver School, New York City
Hawaii Civil Liberties Committee
Hellenic-American Brotherhood
Hollywood Writers Mobilization for Defense
Hungarian-American Council for Democracy
Hungarian Brotherhood
Independent Socialist League
International Labor Defense
International Workers Order, its subdivisions, subsidiaries, and affiliates
Jefferson School of Social Sciences, New York City
Jewish Peoples Committee
Jewish Peoples Fraternal Order
Joint Anti-Fascist Refugee Committee
Joseph Weydemeyer School of Social Science, St. Louis, Mo.
Labor Research Association, Inc.
Labor Youth League
League of American Writers
Macedonian-American People's League
Michigan Civil Rights Federation
Michigan School of Social Science
National Committee for the Defense of Political Prisoners
National Committee to Win the Peace
National Conference on American Policy in China and the Far East (a Conference called by the Committee for a Democratic Far Eastern Policy)
National Council of Americans of Croatian Descent
National Council of American-Soviet Friendship
National Federation for Constitutional Liberties
National Negro Congress
Nature Friends of America (since 1935)
Negro Labor Victory Committee
New Committee for Publications
North American Committee to Aid Spanish Democracy
North American Spanish Aid Committee
Ohio School of Social Sciences
Oklahoma Committee to Defend Political Prisoners
Pacific Northwest Labor School, Seattle, Wash.
Partido del Pueblo of Panama (operating in the Canal Zone)
Peoples Educational and Press Association of Texas
Peoples Educational Association (incorporated under name Los Angeles Educational Association, Inc.) also known as Peoples Educational Center, Peoples University, People's School
People's Institute of Applied Religion
People's Radio Foundation, Inc.
Philadelphia School of Social Science and Art
Photo League (New York City)
Polonia Society of the IWO
Progressive German-Americans, also known as Progressive German-Americans of Chicago
Proletarian Party of America
Revolutionary Workers League
Romanian-American Fraternal Society
Samuel Adams School, Boston, Mass.
Schappes Defense Committee
Schneiderman-Darcy Defense Committee
School of Jewish Studies, New York City
Seattle Labor School, Seattle, Wash.
Serbian-American Fraternal Society
Serbian Vidovdan Council
Slovak Workers Society
Slovenian-American National Council
Socialist Workers Party, including American Committee for European Workers' Relief
Socialist Youth League
Southern Negro Youth Congress
Tom Paine School of Social Science, Philadelphia, Pa.
Tom Paine School of Westchester, New York
Ukrainian-American Fraternal Union
Union of American Croatians
United American Spanish Aid Committee
United Committee of South Slavic Americans
United Harlem Tenants and Consumers Organization
United May Day Committee
United Negro and Allied Veterans of America
Veterans Against Discrimination of Civil Rights Congress of New York
Veterans of the Abraham Lincoln Brigade
Virginia League for Peoples Education
Walt Whitman School of Social Science, Newark, N. J.
Washington Bookshop Association
Washington Committee for Democratic Action
Washington Commonwealth Federation

Wisconsin Conference on Social Legislation
Workers Alliance (since April 1936)
Workers Party, including Socialist Youth League
Yiddisher Kultur Farband
Young Communist League

Subversive:

Alabama Peoples Educational Association
Communist Party, U. S. A., its subdivisions, subsidiaries, and affiliates
Communist Political Association, its subdivisions, subsidiaries, and affiliates
Florida Press and Educational League
German-American Bund
Independent Socialist League
Partido del Pueblo of Panama (operating in the Canal Zone)
Peoples Education and Press Association of Texas
Socialist Workers Party
Virginia League for Peoples Education
Workers Party
Young Communist League

Organizations which have "adopted a policy of advocating or approving the commission of acts of force and violence to deny others their rights under the Constitution of the United States":

American Christian Nationalist Party
Associated Klans of America
Association of Georgia Klans
Columbians
Knights of the White Camellia
Ku Klux Klan
Original Southern Klans, Incorporated
Protestant War Veterans of the United States, Inc.
Silver Shirt Legion of America

Organizations which "seek to alter the form of government of the United State by unconstitutional means":

Alabama Peoples Educational Association
Communist Party, U. S. A., its subdivisions, subsidiaries, and affiliates
Communist Political Association, its subdivisions, subsidiaries, and affiliates
Florida Press and Educational League
Independent Socialist League
Industrial Workers of the World
Nationalist Party of Puerto Rico
Partido del Pueblo of Panama (operating in the Canal Zone)
Peoples Educational and Press Association of Texas
Socialist Workers Party
Virginia League for Peoples Education
Workers Party
Young Communist League

APPENDIX "B"

INSPECTION REPORTS
PETROLEUM AND GAS INDUSTRIES
SECURITY INSPECTION REPORT

INSTRUCTIONS

The security inspection report form is in two parts. Part I, Appendix C, covers a system and Part II, Appendix D, covers individual facilities.

Section A of each part covers general information. The subsequent sections follow the outline of the set of principles providing one general question regarding the adequacy of the security program being inspected in respect to each security element which should be considered. The inspector's answer to these questions is indicated by placing an "X" in the appropriate column opposite each question. If the inspector wishes to comment regarding a particular question, an "X" should also be placed in the "See Comments" column opposite the question and his comments entered in the comments section. Each comment should be numbered and lettered to correspond with the question to which it applies. Where the inspector's answer indicates inadequacy, he must comment.

The inspector's answers regarding the adequacy of the various security elements are expressions of his opinion based upon information he has been able to obtain and his personal observations. In order to assist the inspector in his investigation regarding each question to be answered on the report form, a check list of questions, Appendix E, has been prepared following the same outline as the report and including points brought out by the manual. The check list provides several questions to be considered before the adequacy of a particular item in the report is determined. This check list is a guide for the inspector and he is not necessarily limited to these questions.

An inspection should begin with the inspector contacting top management. The official responsible for security will be able to provide the inspector with information on the over-all security program. "Part I—System Report" covers this phase of the inspection, but should not be completed until the inspector has had an opportunity to verify the information received by inspecting certain individual facilities. The official responsible for security will usually designate a representative to accompany the inspector during his inspection of the individual facilities. "Part II—Individual Facility Report," should be prepared for each facility inspected. The inspector should discuss his findings and recommendations with the official responsible for security or his designated representative before completing the report forms.

The "A—GENERAL INFORMATION" sections of the report form are generally self-explanatory, but in case questions should arise, explanations of various items are as follows:

Part I—System Report (A—General Information)

1. Self-explanatory.
2. Self-explanatory.
3. Self-explanatory.
4. Self-explanatory.
5. This item covering the official responsible for security is intended to show the person to whom future correspondence should be addressed or contacts made regarding security.
6. Self-explanatory.
7. This item covering capacity, products, etc., is primarily to provide information as to the size of the system inspected and the scope of its operations. Therefore, approximate figures will suffice.
8. The remarks item should be used to cover any pertinent information that has not been provided for on the form. For example, the date of the next recommended inspection, labor organizations, if any, criticality rating, etc.

Part II—Individual Facility Report (A—General Information)

1. If the facility is in a remote area, its location in respect to an easily identified location should be given.
2. Self-explanatory.
3. Self-explanatory.
4. This section is to provide information as to the size of the facility inspected and the scope of its operations. Therefore, approximate figures will suffice.
5. Self-explanatory.
6. Self-explanatory.
7. The remarks section should be used to cover additional pertinent information, such as construction in progress to increase capacity, the schedule for new units, the date of next recommended inspection, criticality rating, etc.

APPENDIX "C"

PETROLEUM AND GAS INDUSTRIES

SECURITY INSPECTION REPORT

PART I

SYSTEM REPORT

Army Area ..... Report Prepared By .....

Naval District ..... Date of Inspection .....

Air Force Command ..... Date of Last Inspection.....

A—GENERAL INFORMATION

1. Name of Company .....

   Mail Address .....

2. State of Incorporation.....Common Carrier Yes ( ) No ( )

3. Subsidiary of .....

4. Names and Titles of Principal Officials:

.....

.....

.....

.....

5. Official Responsible for Security

.....

6. Attach System Map

7. a. Maximum Throughput Capacity .....

   b. Types of Products Handled .....

   c. States Traversed by Pipe Line .....

8. Remarks (Use Extra Sheets If Needed)

.....

.....

.....

.....

.....

.....

.....

.....

.....

APPENDIX "C" (cont'd)

B–PROTECTIVE MEASURES

	Adequate	Inadequate	See Comments
1. Selection of Vital Facilities			
2. Determination of Restricted Areas			
3. Organization			
4. Personnel			
5. Access Control			
6. Safeguarding Classified Security Matter			
7. Protection and Duplication of Records			
8. Security Liaison			
9. Employee and Public Relations			
10. Inspections and Reports			
11. Guard Service			
12. Fencing and Other Anti-Personnel Barriers			
13. Protective Lighting			
14. Protective Alarm Systems			
15. Communications			
16. Fire Protection			
17. Safety			
18. Miscellaneous Considerations			
19. Blast Barriers			
20. Camouflage			
21. Blackouts and Dimouts			
22. Bomb Shelters			
23. Civil Defense Aspects			
24. Restoration of Production or Service			

Comments and Recommendations (Use Extra Sheets If Needed)

APPENDIX "D"

PETROLEUM AND GAS INDUSTRIES

SECURITY INSPECTION REPORT

PART II

INDIVIDUAL FACILITY REPORT

Army Area ..... Report Prepared By .....

Naval District ..... Date of Report .....

Air Force Command ..... Date of Last Inspection.....

A–GENERAL INFORMATION

1. Name of Facility .....
   Mail Address .....
   Location .....

2. Parent Company .....
   Mail Address .....

3. Type of Facility .....

4. (a) Petroleum Facility Tankage Pipe Line

Product	Storage Capacity	Current Throughput	Maximum Capability
Aviation Gasoline			
Motor Gasoline			
Kerosene & Range Oil			
Light Fuel Oils			
Heavy Fuel Oils			
Lubricating Oils			
Crude Oil			
Others			
TOTAL			

   (b) Gas Facility
      1. Daily Peak Load Capacity.....
      2. Daily Normal Capacity.....
      3. Daily Maximum Capacity.....

5. Names and Titles of Principal Officials:

.....

.....

.....

6. Official Responsible for Security:

.....

7. Remarks (Use Extra Sheets If Needed)

.....

.....

.....

.....

APPENDIX "D" (cont'd)

B–PROTECTIVE MEASURES

	Adequate	Inadequate	See Comments
1. Selection of Vital Facilities			
2. Determination of Restricted Areas			
3. Organization			
4. Personnel			
5. Access Control			
6. Safeguarding Classified Security Matter			
7. Protection and Duplication of Records			
8. Security Liaison			
9. Employee and Public Relations			
10. Inspections and Reports			
11. Guard Service			
12. Fencing and Other Anti-Personnel Barriers			
13. Protective Lighting			
14. Protective Alarm Systems			
15. Communications			
16. Fire Protection			
17. Safety			
18. Miscellaneous Considerations			
19. Blast Barriers			
20. Camouflage			
21. Blackouts and Dimouts			
22. Bomb Shelters			
23. Civil Defense Aspects			
24. Restoration of Production or Service			

Comments and Recommendations (Use Extra Sheets If Needed)

APPENDIX "E"

CHECK LIST FOR PETROLEUM OR GAS SYSTEM AND FACILITY SECURITY INSPECTION

1. SELECTION OF VITAL FACILITIES

a. Has management made a study of the critical and vulnerable points in the system or facility?

b. What criteria are used?

c. Are these determinations reviewed periodically?

d. What steps are taken to give special protection to these vital areas?

e. What steps are taken to reduce criticality and vulnerability, where possible?

2. RESTRICTED AREAS

a. Have vital areas in the system or facility been restricted?

b. Is access to restricted areas limited to authorized individuals?

c. What protective measures are established with respect to restricted areas?

d. Are escort procedures established?

3. ORGANIZATION

a. Has an individual or group been placed in charge of a security program?

b. Do employees have adequate representation on the security staff?

c. Has the security staff surveyed the system or facility and studied the security problems involved?

d. Is there a plan covering all phases of security?

e. Is the security staff adequate to carry out its responsibility?

f. Is the security staff prepared to train employees in their duties, including emergency duties?

g. Are provisions made to test the security plan and program?

4. PERSONNEL

a. (1) How are employees instructed in security matters?

(2) Does the method used provide continuous training?

(3) Does the method used produce the desired results?

(4) Does the training include the elements listed on page 22 of the manual?

(5) Are employees instructed to report all suspicious acts or persons?

b. (1) Are all employees given loyalty investigations?

(2) If not, are all key employees investigated?

(3) What type of loyalty investigations are made?

(4) Who conducts the loyalty investigations?

(5) Are special background investigations made for employees who have access to classified security matter?

(6) Are non-employees who require access to restricted areas investigated?

(7) Is special attention given to alien employees and applicants?

5. ACCESS CONTROL (of admission to restricted areas)

a. (1) Does the access control procedure provide for positive identification?

(2) Does it provide a positive means of determining authority to admit?

(3) Are special precautions taken at access gates during hours of darkness, particularly at other than shift change periods?

(4) At night is the guard exposed to observation from outside the gate when examining credentials of persons desiring access? If so, is he alone?

b. (1) Are employees' badges and identification cards used? If so, are they tamperproof in design?

(2) Are controls applied to account for those on hand and to recover passes and badges upon expiration or when no longer required?

(3) How are contractors' employees controlled? Do they wear distinctive badges?

(4) Do guards carefully compare individuals to their identifying device before admitting them?

c. (1) Are visitors provided distinctive badges or passes?

(2) Are visitors escorted?

(3) Is a visitor register maintained?

6. CLASSIFIED SECURITY MATTER

a. Do only authorized personnel have access to classified matter?

b. Are proper cabinets provided to store classified matter?

c. Are copies of security matter properly controlled and protected?

d. How is classified matter disposed of when no longer needed?

7. PROTECTION OF RECORDS

a. Are important records well stored?

b. Have vital records been microfilmed and safely stored?

c. Do limited number of people have access to records?

8. SECURITY LIAISON

Have following agencies been contacted: Department of Defense, Federal Bureau of Investigation, local Civil Defense organization, police and fire departments?

9. EMPLOYEE AND PUBLIC RELATIONS

a. What measures have been taken to enlist support of employees and public in security program?

b. Do employees have representation in development of security program?

c. Are labor groups informed of need for security program? Is their support requested?

10. INSPECTIONS AND REPORTS

a. What system of inspection is used?
b. How often are they made?
c. Does management make inspections?
d. Are outside experts used in making inspections?
e. Are employees designated to make inspections?
f. What phases of the security program are covered in inspections?
g. Who receives results of inspections?
h. What action is taken as result of inspections?

11. GUARD SERVICE

SYSTEM

a. Are all restricted areas guarded?
b. Are all guards investigated?
c. How is the guard system organized?
d. How are guards trained?
e. What are guard qualifications?
f. How are guards armed?
g. What kind of uniform or identification do they have?
h. Are guards properly supervised when on duty?

FACILITY

a. Are the number of guard posts adequate to provide proper control at the access points and at the same time give adequate coverage to the perimeter barrier?
b. Are guard posts varied each time the guards come on duty?
c. Are test exercises held of emergency operations?
d. Are guards thoroughly familiar with their duties?
e. What kind of communications system is there for use of guards?
f. Are guard posts located so as to keep the guard in the darkened area behind the protective lighting screen at night?
g. Are guard shelters designed to provide maximum assistance to the guard?

12. FENCING AND ANTI-PERSONNEL BARRIERS

a. Is the vital area completely enclosed by a cyclone fence or equal barrier?
b. If the facility is very critical, is there a close-in as well as an outer barrier?
c. Has due consideration been given to emergency entrances and fire exits?
d. If there is a water approach to the facility, is this approach properly protected?
e. Have both sides of the fence been cleared of underbrush, equipment, etc.?
f. Are openings, such as windows, air ducts, sewers, tunnel entrances, properly barricaded?

13. PROTECTIVE LIGHTING

a. Are vital areas covered by protective lighting?
b. Is the protective lighting arranged so as to light up all approaches to facility?
c. Are guard posts and vital areas located behind the light beam?
d. Are there alternate sources of power for lighting?

14. PROTECTIVE ALARM SYSTEM

a. What type of system is used?
b. Are signals received at a central station with a guard in attendance at all times?
c. Can guards quickly reach all areas after alarm is sounded?
d. Are any important areas left uncovered?
e. Is the general purpose served of reducing use of other protective elements and yet providing reasonable protection?

15. COMMUNICATIONS

a. Does the communications system provide comprehensive coverage of facility?
b. Are there alternate means of communications?
c. Are there communications between the facility and sources of outside help, such as Civil Defense, police, medical, etc.?
d. Is the equipment tested periodically?

16. FIRE PROTECTION

a. Is a fire manual or fire regulations provided and kept up to date?
b. Is there an adequate program of housekeeping and fire prevention?
c. Are periodic inspections made of fire-fighting equipment?
d. Are employees properly trained in the use of fire-fighting equipment and in their duties in the event of fire?
e. Have arrangements been made with the local fire department for help when needed?

17. SAFETY

a. Is an adequate safety organization established?
b. Are employees represented on this organization?
c. Is there an adequate safety education program?
d. Is proper supervision made of conditions?
e. Are protective equipment and clothing provided?
f. Are first-aid and medical facilities provided?
g. Are records evaluated to determine effectiveness of program?

18. MISCELLANEOUS CONSIDERATIONS

Have miscellaneous measures to protect facility, such as vehicle control, package control, protection of power supply, dispersion, etc., been considered?

19. BLAST BARRIERS

a. Are blast walls or barriers located around vital equipment?

20. CAMOUFLAGE

a. Have military authorities advised use of camouflage?
b. Have they made specific recommendations?
c. Are these recommendations being complied with?

21. BLACKOUTS AND DIMOUTS

a. Are blackouts or dimouts of any use?
b. Who has recommended them?
c. What has been recommended?
d. Are these recommendations being followed?

22. BOMB SHELTERS

a. Have buildings been surveyed by qualified engineers to determine best shelter areas?

b. Are shelters away from danger of flying glass, heavy overhead weights and concentrations of steam or gas pipes or electric conduits?

23. CIVIL DEFENSE ASPECTS

a. Has one individual been placed in charge of civil defense program?

b. Have groups been formed to provide necessary services, such as first-aid, fire-fighting, rescue, etc., in the emergency?

c. Does plant have an effective warning system, including arrangements to receive warning from local Civil Defense?

d. Have shelter areas been designated? Are they clearly marked?

e. Has liaison been established with local Civil Defense organization?

f. Is there a well protected control center?

g. Have air raid drills been held?

h. Have employees been trained in self-protection?

i. Have employee groups been trained in their emergency duties?

j. Have test exercises been held to test effectiveness of organization?

24. RESTORATION OF PRODUCTION OR SERVICE

a. *Organization*

(1) Is there a general organization plan for emergencies and disaster?

(2) Are alternates for key personnel designated?

(3) Is there an adequate emergency communication system?

(4) Is there an adequate emergency system for the transport of personnel to required places?

(5) Have alternate headquarters for emergency operation been provided?

(6) Is there provision for adequate liaison and coordination with associated agencies including military and civil defense groups?

b. *Personnel*

(1) Have regular operating personnel been instructed in the extension of their normal duties required for protection against enemy action?

(2) Has provision been made to reinforce normal operating personnel during emergency with employees of other departments?

(3) Do arrangements exist for the utilization of personnel of other power supply and related construction organizations if required in an emergency?

c. *Training*

(1) Are regular operating personnel trained for emergency and disaster contingencies?

(2) Is there an adequate program for training non-operating personnel in assigned duties?

d. *Equipment and Tools*

(1) Are equipment and tools dispersed?

(2) Have arrangements been made for emergency procurement from suppliers?

(3) Are there arrangements for securing equipment and tools from other power supply organizations?

e. *Records*

(1) Have essential records been duplicated and dispersed?

f. *Auxiliary Supporting Services*

(1) Is there provision for furnishing temporary living quarters for personnel if required?

(2) Is there provision for medical aid during the emergency?

(3) Are adequate building maintenance services provided for operating headquarters establishments?

(4) Is adequate emergency police protection provided?

(5) Have maintenance personnel for communication, electrical and plumbing facilities been provided?

(6) Has a messenger service been provided?

(7) Has an auxiliary organization for the aid of employees' families been set up?

(8) Is there adequate provision for gassing, lubrication and maintenance of transport?

g. *Testing the Plan*

(1) Have representative damage problems been developed?

(2) Have emergency communications systems been proved?

(3) Have there been test exercises in manning emergency headquarters?

(4) Is the plan adapted to function with local control if necessary?

h. *Selective Restoration*

(1) Are key personnel indoctrinated in this principle?

(2) Have all vital community facilities been made known to key personnel and lists provided where required?

(3) Have tentative priorities been determined among these vital elements?

i. *Additional*

(1) Is a list of key individuals in adjoining utilities and Government Agencies maintained showing how they may be reached?

(2) Are alternate power supplies and interconnections with other systems provided?

(3) Are small planes or helicopters available for assessment of damage and observation?

(4) Have radiological teams, damage survey and debris clearance crews been organized?

(5) Have provisions been made for transmitting appropriate vital information to the public?

(6) Have cash credits been established in decentralized locations?

(7) Has a mobilization procedure been established?

(8) If so, does it provide for alerting all key personnel promptly and are all such persons properly instructed regarding their duties when alerted?