NUREG/CR-1385
SAND80-7027
Unlimited Release

Development of a "Good" Physical Protection Plan - Capability 73.45(b)

Harold A. Bennett, M. Teresa Olascoaga, Sandia National Laboratories
Steve A. Bloedel, Allied General Nuclear Services

Printed March 1980

Sandia National Laboratories

Prepared for
U. S. NUCLEAR REGULATORY COMMISSION

NOTICE

The views expressed in this report are not necessarily those of the U. S. Nuclear Regulatory Commission

Available from

GPO Sales Program
Division of Technical Information and Document Control
U.S. Nuclear Regulatory Commission
Washington, D.C. 20555

and

National Technical Information Service
Springfield, Virginia 22161

NUREG/CR-1385
SAND80-7027
Unlimited Release

DEVELOPMENT OF A "GOOD" PHYSICAL PROTECTION PLAN - CAPABILITY 73.45(b)

H. A. Bennett, M. T. Olascoaga
Sandia National Laboratories
Albuquerque, NM 87185

S. A. Bloedel
Allied-General Nuclear Services
Barnwell, SC 29812

Date Published: March 1980

Submitted by
Allied-General Nuclear Services
Barnwell, SC 29812
under
Contract Document No. 13-7145
to
Sandia National Laboratories
Albuquerque, New Mexico 87185
operated by
Sandia Corporation
for the
U.S. Department of Energy

Prepared for
Division of Safeguards
Office of Nuclear Material Safety and Safeguards
U.S. Nuclear Regulatory Commission
Washington, DC 20555
Under Interagency Agreement DOE 40-550-75
NRC FIN No. A1153

ABSTRACT

This report describes the development and documentation of a partial physical protection plan for a hypothetical facility. This work, performed by Allied-General Nuclear Services under contract to Sandia Laboratories, provides limited testing of the NRC Fixed-Site Physical Protection Upgrade Rule Design Guidance Compendium and of a methodology for evaluating physical protection system performance relative to the Upgrade Rule, 10 CFR Part 73.45.

TABLE OF CONTENTS

TABLE OF CONTENTS (CONTINUED)

1.0 EXECUTIVE SUMMARY

This study has exercised a portion of the Design Guidance Compendium to determine its completeness, validity, and utility, respective of its capacity to aid the licensee in designing a Physical Protection System. Unequivocally, the Design Guidance Compendium possesses invaluable attributes which facilitate and enhance the development of a Physical Protection System complying with the requirements of the Physical Protection Upgrade Rule (10 CFR 73.45). Significant attributes include:

(1) The paramount attribute of the Design Guidance Compendium is an inherent characteristic to continuously subject the licensee to an evaluation of the total Physical Protection System. As each new component or system is added to the total system, the licensee becomes initially exposed to both the beneficial and detrimental characteristics of the component. Subsequently, this exposure broadens and necessitates the licensee to evaluate both the impact of the component on the Physical Protection System and the impact of the Physical Protection System on the component. The principal benefit of this exercise is the continuous self-test capability afforded by the Design Guidance Compendium which identifies component inadequacies and system incongruencies.

(2) A second attribute of the Design Guidance Compendium is a responsiveness to the needs of the licensee to evaluate the effectiveness of the Physical Protection System in complying with the requirements of the Physical Protection Upgrade Rule. As components are added to the total system, the licensee evaluates the performance levels of the component. The licensee is, therefore, afforded the opportunity to compensate for minimal performance levels by one component by elevating the performance levels of components which interact within the same physical protection subsystem. This attribute is extremely valuable to currently operating facilities which are, by design, restricted to certain types of physical protection system designs.

(3) The third major attribute of the Design Guidance Compendium is the establishment of conformity in the licensing process. By responding to the information solicited in the Design Guidance Compendium, the licensees are committed to the submission of security plans which are more cohesive and coordinated. These Physical Protection Plans will contain, and be limited to, only the information necessary to perform a thorough evaluation of the physical protection systems' performance capabilities. Additionally, the licensees are relieved of the responsibility of determining the types of

information required, since the Design Guidance Compendium identifies the criteria from which the Physical Protection System and the associated Physical Protection Plan are evaluated.

The only notable deficient area of the Design Guidance Compendium focuses upon consistency between the information requested by the Information Request Sheet and the information evaluated by the associated Effectiveness Test Questionnaire. Generically, information concerning a specific component or system is requested and then not evaluated or information is evaluated, but never requested. Additionally, identical information for similar components or systems is not always requested or evaluated. However, these negative aspects are minimal when compared to the positive attributes of the Design Guidance Compendium.

In conclusion, the benefits which can be derived from the implementation of the Design Guidance Compendium are invaluable. Maximization of Design Guidance Compendium utility occurs when the compendium is implemented during the design phase of the facility, e.g., concurrently with health and safety, operations, and maintenance design considerations. However, the reliability of all fixed nuclear facility physical protection systems, whether planned, being constructed, or operating, is sufficiently enhanced by operationalizing the requirements of the Design Guidance Compendium into the facility's Physical Protection System to warrant its implementation.

2.0 INTRODUCTION

Allied-General Nuclear Services (AGNS), under Contract No. 13-7145 with Sandia Laboratories, has prepared this report to assist Sandia and NRC in implementing and testing a portion of the Physical Protection System Design Guidance and Performance Evaluation Methodology. These exercises are pursuant to determining the completeness, validity, and utility of the Design Guidance Compendium with respect to aiding the fixed nuclear facility licensee to design a Physical Protection System which satisfies the requirements of the Physical Protection Upgrade Rule (10 CFR 73). The following objectives were addressed:

(1) Utilizing the Design Guidance Compendium, a "good" partial Physical Protection Plan which complies with the performance capability specified in 10 CFR 73.45(b) has been developed and documented. The facility being protected encompasses an MAA, containing a single vault, which is totally enclosed within the confines of a Vital Area (VA). The plan is comprised of two parts. First, the AGNS Sample Plan, a generic description of the Physical Protection System, contains information dealing with specific parts of the total Physical Protection System, including identification of components incorporated into the system and responses to specific regulatory requirements. The second part is composed of Information Request Sheets (IRS) which support the generic Physical Protection System description. These IRS forms provide specific, technically oriented information pertinent to the rationale for selection and utilization of the components in the Physical Protection System.

(2) Effectiveness Test Questionnaires (ETQ) associated with each component identified within the context of the generic description of the Physical Protection System have been completed. These answers will be utilized by Sandia to quantitatively evaluate the degree of compliance exhibited by the "good" partial Physical Protection Plan in complying with the requirements of 10 CFR 73.45(b).

(3) Based upon the experience and expertise gained during the completion of the above, a documented critique of the Design Guidance Compendium was provided. The critique is intended to illustrate both the weak and strong points of the compendium with respect to its ability to aid the licensee in designing a Physical Protection System and in preparing the associated license document which satisfy the performance requirements of the NRC.

3.0 PARTIAL PHYSICAL PROTECTION PLAN

"AGNS' SAMPLE PLAN"

The Standard Format and Content Guide of the Design Guidance Compendium is segregated into 23 chapters. Chapters 1 through 17 provide an overview of the Physical Protection System and address topics relevant to the entire Physical Protection Plan. Chapters 18 through 23 parallel the performance capabilities of the Physical Protection Upgrade Rule by generically describing how the capabilities are achieved and by identifying the procedures, components, and systems implementing the capability. The "AGNS Sample Plan" illustrates the development of a "good" partial Physical Protection Plan corresponding to the performance capability requirements specified in Chapter 18 of the Standard Format and Content Guide.

Throughout "AGNS' Sample Plan" procedures, components, and systems utilized to implement the performance capability are associated with a unique reference number (Reference XX-XX). These reference numbers identify Information Request Sheets (see Section 4.0) which provide detailed, technical information supporting the use of the component, system, or procedure in the sample plan. The first set of numbers identifies the category of information with respect to the "List of Information Request Sheet Titles" contained in the Design Guidance Compendium. The second set of numbers identifies the sequential number of the Information Request Sheet with respect to its appearance in the Physical Protection Plan. For example, in Reference 6-1 the "6" indicates the Information Request Sheet contains information about a balanced magnetic switch. The "1" indicates that this is the first type of balanced magnetic switch to be discussed in the plan.

18.0 PREVENT UNAUTHORIZED ACCESS OF PERSONS, MATERIALS, AND VEHICLES

This section describes the components, systems, and procedures utilized to ensure attempts by personnel to gain unauthorized access and/or to introduce unauthorized materials are detected, assessed, and communicated. All attempts, either by stealth, force, or deceit, result in a timely response initiated to deter, delay, or deny the unauthorized access or penetration. These entry controls satisfy the performance capability requirements of 10 CFR 73.45 (b).

18.1 Portal Entry Control

Figure 18-1 identifies the MAA, the vault, and the associated portals. One entry/exit point, designated MAA-1.1 (Reference 21-1), penetrates the east wall and one emergency exit, designated MEE-1.1 (Reference 28-1), penetrates the north wall of the MAA. One entry/exit point, designated VAU-1.1 (Reference 21-1), penetrates the south wall of the vault (Reference 86-1).

18.1.1 Entry Authorization Procedures

Entry authorization verification procedures (Reference 2-1) limit controlled access area admittance to only those personnel authorized to perform specifically assigned tasks and at only those times when the performance of these activities is authorized. Authorization Schedules (Reference 1-1), derived from Shift and Production Schedules, determine what activities are authorized and when, and by whom, these activities are conducted. Entry authorization verification procedures progressively become more restrictive as the sensitivity of the controlled area increases.

18.1.1.1 Entry Authorization

Entry authorization consists of a computerized criteria screening process. This process compares area access criteria, contained in the Area Authorization File (AAF), against personnel access qualifications, contained in the Personnel Authorization File (PAF). Area access criteria includes administrative and security requirements, the category of activities requested (Work Designation Codes, Table 18-1), and the periods these activities are authorized (Production Schedule). Personnel access qualifications include the category of activities an individual is authorized to perform (Work Designation Codes), the periods the individual is authorized to perform these activities (Shift Schedule), and the administrative and security requirements possessed by the individual.

18.1.1.2 Personnel Entry Authorization

Personnel entry authorization is automatically initiated and verified each time an individual requests admittance to a controlled access area.

18.1.1.3 Maintenance and Distribution of Entry Authorization

Personnel entry authorization is maintained current by continuously updating the Personnel Authorization File (PAF) and the Area Authorization File (AAF). No two individuals are capable of programming the PAF with sufficient data to authorize an individual admittance to a controlled access area. Similarly, personnel authorized to program the AAF with area access criteria do not have access to the PAF.

Personnel entry authorization information is displayed on computer communication terminals located in manned entry control points and at the Central Alarm Station (CAS) and the Secondary Alarm Station (SAS).

The CAS and the SAS have the capability of displaying a list of all personnel currently occupying a controlled access area and a record of all entry and exit events which have occurred within the last 24 hours.

18.1.2 Entry Procedures and Controls

The incorporation of security officers and entry control systems and procedures serves to maximize the probability of detecting unauthorized persons, contraband, and unauthorized vehicles attempting to enter a controlled access area. These measures are applied during both routine (Table 18-2) and nonroutine conditions.

18.1.2.1 Routine Conditions

Table 18-3 identifies generic criteria which govern access functions during routine working and nonworking conditions; excluding nonroutine conditions which are identified in Section 18.1.2.2.

18.1.2.1.1 Procedures and Controls for Personnel Entry

Personnel entry controls and procedures are designed and operated in a manner which verifies admittance authorization and positive personnel identification prior to authorizing admittance into the MAA Secured Access Portal (SAP) (Reference 68-1) and the MAA, respectively. These controls guarantee that access to an MAA shall include at least two individuals. All admittance search functions are conducted within the MAA SAP which is isolated from both the MAA and the PA. This admittance concept maximizes the integrity of the MAA until access authorization and personnel identification are verified and provides containment of personnel until all admittance search functions have been satisfactorily

completed. It also facilitates containment of personnel by security officers should suspicious activities be observed within the MAA SAP.

Vault entries require additional authorization, but do not require additional search or identification measures.

18.1.2.1.1.a Secured Access Portal Operations

MAA SAP and MAA Entry

The following steps are performed by the individual desiring access unless otherwise specified:

- Step 1 - Note the condition of the red light located next to the MAA SAP proximity reader. If the light is "off," pass the Coded Credential Badge (Reference 14-1) in front of the proximity reader. If the red light is "on," indicating admittance functions are in progress, wait until the light is de-energized.

  Passing the Coded Credential Badge in front of the proximity reader signals the control processor to initiate a search of the PAF and the AAF to determine if MAA SAP access is authorized. Authorization de-energizes an electronic door strike opening one of two MAA SAP door locks and keys the Voice Verification System (VVS) (Reference 65-1). The second door lock is normally open. This door lock, operated by the security officer inside the MAA SAP, prevents MAA SAP entry while admittance operations are in progress.

- Step 2 - Enter the MAA SAP and close the entrance door.

  This action enrolls the individual on the Personnel Inventory System as being within the MAA.

- Step 3 - The security officer, after ensuring the MAA SAP entrance door is closed and that only one person entered the MAA SAP (two for an initial entry during any work period or if one requires an escort), actuates the second MAA SAP entrance door lock.

  This action prevents MAA SAP entry while admittance functions are in progress and energizes the red light next to the proximity reader.

- Step 4 - Inside the MAA SAP, establish positive personnel identification by responding to the requests of the VVS minicomputer.

- Step 5 - The security officer, after positive personnel identification has been verified, performs a sequence of contraband search functions on the individual requesting admittance.

- Step 6 - The security officer, having completed the contraband search, inputs the control processor indicating successful completion of the contraband search and requests the CAS or the SAS to actuate the MAA-1.1 door lock.

- Step 7 - The CAS or the SAS, verifying that only one person passes through MAA-1.1 by CCTV (Reference 11-1), de-energizes an electronic door strike opening one of two MAA-1.1 door locks.

- Step 8 - While the door strike is de-energized, pass the Coded Credential Badge in front of the MAA proximity reader. The control processor, after verifying positive personnel identification, successful completion of the contraband search, and MAA access authorization, de-energizes the second of two door locks permitting MAA admittance.

- Step 9 - The security officer, after the individual has entered the MAA, closes MAA-1.1.

- Step 10 - The security officer de-energizes the second MAA SAP door lock allowing MAA SAP admittance and de-energizing the red light.

Vault Entry

The following steps are performed by the individual desiring access unless otherwise specified:

- Step 1 - Pass the Coded Credential Badge (Reference 14-1) in front of the vault proximity reader.

  This action signals the control processor to initiate a search of the PAF and the AAF to determine if vault access is authorized, and alerts the CAS, the SAS, and the security officer in the MAA SAP that a vault entry has been requested. Authorization de-energizes an electronic door strike opening one of two VAU-1.1 door locks.

- Step 2 - The CAS or the SAS, verifying that only one person passes through VAU-1.1 by CCTV (Reference 11-1), de-energizes an electronic door strike opening the second of two door locks permitting vault entry. Verification is also provided by a CCTV monitor (Reference 11-1) located in the MAA SAP.

- Step 3 - Enter the vault and close VAU-1.1.

  This action enrolls the individual on the Personnel Inventory System as being within the vault and removes the individual from the MAA inventory listing.

- Step 4 - The CAS and the SAS ensure VAU-1.1 is closed.

This step is accomplished by observing that the alarm, generated by the balanced magnetic switch (Reference 6-1) monitoring VAU-1.1, de-energizes.

18.1.2.1.1.b I.D. Verification and Authorization

Entry authorization utilizes a Coded Credential Badge system (Reference 14-1). When an individual requests access to a controlled access area, the credential system's control processor automatically scans the PAF and the AAF and verifies that the individual to whom the Coded Credential Badge was issued is authorized entry. The employee's name, employee number, and Work Designation Codes (Tables 18-1 and 18-7) are also displayed on the MAA SAP computer communications terminal.

Positive personnel identification utilizes a Voice Verification System (VVS) (Reference 65-1). When an individual enters the MAA SAP, the VVS minicomputer requests the individual to repeat a randomly selected sequence of four prerecorded words. Positive personnel identification is verified by an acceptable response from the individual requesting admittance.

18.1.2.1.1.c Personnel Escort

Reference 31-1 describes the procedures and policies for escorting visitors within a MAA and a vault.

18.1.2.1.1.d Contraband Detection

The purpose of contraband detection is to identify the introduction of unauthorized materials into a MAA or vault. These detectors possess a moderate to high degree of sensitivity and medium throughput. Because the vault is located within the MAA, a search for contraband is only required for access to the MAA.

Metal Detection (Table 18-4)

Metal detectors are capable of detecting weapons and hand tools and the presence of metal utilized for shielding SNM. Because higher frequency range metal detectors possess the highest sensitivity to small amounts of metal, an active metal detection system was selected. Both walkthrough (Reference 72-1 and 95-1) and hand- held (Reference 92-1) metal detectors are used.

Explosive Detection (Table 18-5)

Specificity is a critical factor when selecting an explosives detector. The SAP is manned by security officers trained to differentiate between different types of explosives initiating an alarm. Resultantly, hand-held explosive detectors, with moderate to low specificity and moderate to high sensitivity, are employed (Reference 33-1).

Nuclear Material Detection (Table 18-6)

Because it is possible to defeat a SNM detector by shielding the material, the above referenced metal detectors (Reference 72-1 and 92-1) are utilized in conjunction with the SNM monitor. Hand-held monitors were selected because of their greater sensitivity for detecting nuclear material than doorway type monitors (Reference 74-1).

As an entry control component, the SNM detector functions to prevent the introduction of substitute nuclear materials. As an exit control component, the SNM detector functions to prevent the unauthorized removal of SNM.

18.1.2.1.1.e Response to Suspected Unauthorized Personnel

MAA

Requesting admittance to a MAA's SAP with a Coded Credential Badge which has been issued to an individual not possessing MAA admittance authorization automatically alerts the CAS, the SAS, and the security officer inside the MAA SAP of the attempted entry. The response is in accordance with Chapter 23 of this plan.

During admittance operations, should positive identification of an individual be questioned, contraband detected, or the activities of the individual warrant suspicion, the security officer does not indicate his concern to the individual. Instead, the security officer continues and prolongs the admittance operation until response personnel arrive at the MAA SAP. The security officer reports this situation to the CAS and the SAS in accordance with Chapter 23 of this plan.

Vault

Requesting admittance to the vault with a Coded Credential Badge which has been issued to an individual not possessing vault admittance authorization automatically alerts the CAS, the SAS, and the security officer inside the MAA SAP of the attempted entry. The response is in accordance with Chapter 23 of this plan.

18.1.2.1.2 Procedures and Controls for Introduced Materials

SNM entering or exiting the MAA and the vault is always confined to the various piping systems appropriate to the type of transfer operation. Resultantly, only maintenance- and operations-related materials, subject to periods when such activities are authorized, are authorized admittance to the MAA or the vault. Additionally, a predetermined inventory of frequently required tools, emergency first aid equipment, and materials which are required, but could also be utilized for sabotage, are maintained within

the MAA to minimize the introduction of materials through the MAA SAP.

Materials are always searched after the individual requesting admittance has successfully completed all admittance search functions.

18.1.2.1.2.a Verification and Material Identification

Individuals desiring to introduce materials into a MAA or vault are required to submit a Security Work Order (SWO) (Reference 98-1) to the Security Supervisor prior to MAA SAP entry. The SWO specifically identifies each component to be introduced. The Security Supervisor authorizes the material by checking the Production Schedule, assigns the SWO an identification number, files the original, and gives the individual a copy. The SWO is then entered into the computer communications central storage file. When the materials are presented for introduction, the security officer retrieves the inventory listing by inputting the computer communications terminal with the SWO identification number. The security officer then checks the inventory listing against the materials being introduced to ensure only authorized materials are admitted.

18.1.2.1.2.b Material Inspection and Monitoring

Materials are searched for contraband utilizing those measures identified in Tables 18-4 through 18-6. All boxes, parcels, and packages are opened and inspected for concealed, unauthorized materials while within the MAA SAP. Instrumentation and other similar components are checked to verify that tamper seals are authentic and that they have not been violated (Reference 83-1).

18.1.2.1.2.c Response to Unauthorized Materials

In the event material is presented for admittance to the MAA, or the vault which is not listed on the SWO's inventory listing, or if contraband is detected, the security officer does not indicate his concern to the individual. Instead, the security officer continues and prolongs the admittance operation until response personnel arrive at the SAP. The security officer reports the situation to the CAS or the SAS in accordance with Chapter 23 of this plan.

18.1.2.1.3 Procedures and Controls for Vehicle Entry

Facility configuration makes vehicle entry to the MAA or the vault impossible under all credible conditions.

18.1.2.2 Nonroutine Conditions

Nonroutine conditions are comprised of one or more categories of postulated incidents or various nonroutine production and/or environmental conditions. Postulated incidents are identified in the Site Emergency Plan. During the initial stages of a nonroutine condition, the exact status within the controlled area may not be known. However, to cope with the nonroutine condition in a manner which satisfies both the physical protection and emergency planning performance objectives, a mutually beneficial blending of both planning concepts is required. Table 18-7 identifies nonroutine conditions and associated Work Designation Codes.

18.1.2.2.1 Verification of Nonroutine Conditions

The authenticity of a nonroutine condition is verified in accordance with the Contingency Plan and Procedures (Reference 16-1). Verification of the condition is commmunicated to all Security personnel in accordance with Chapter 23 of this plan.

18.1.2.2.2 Nonroutine Entry Authorization

The need for nonroutine admittance to a controlled area cannot be anticipated during the preparation of a Production Schedule. Consequently, the AAF is updated continuously and as necessitated by the occurrence of such activities.

Emergency Conditions

Individuals assigned to the various emergency response teams have Emergency Work Designation Codes (Table 18-7) added to their personal access qualifications. When an emergency occurs and its authenticity verified, the AAF is immediately updated with the Emergency Work Designation Codes of required emergency response teams so as to authorize appropriate response personnel access to the controlled area. Programming the AAF with Emergency Work Designation Codes also cancels all routine work access authorization for the affected area until the emergency condition terminates.

Production and Environmental Conditions

When these nonroutine conditions occur and their authenticity is verified, the AAF is updated with Production or Environmental Work Designation Codes to authorize access to those individuals required to mitigate or correct the situation. Normally, access would be authorized to operations personnel for production perturbations and extended to maintenance personnel for environmental problems. Programming the AAF with Production or Environmental Work Designation Codes does not automatically cancel routine work access authorization. However, routine work

cancellation may be an appropriate response alternative until the nonroutine condition terminates.

18.1.2.2.3 Procedures and Controls for Personnel Entry

Entry procedures and controls specified in 18.1.2.1.1 are applied to all personnel desiring access to the MAA or the vault, except personnel possessing an A1 (fire) and A2 (personnel injury) Emergency Work Designation Code (Table 18-7).

18.1.2.2.3.a Secured Access Portal Operations

Personnel Injury

A2 designated personnel responding to a personnel injury individually request admittance to the MAA SAP by passing their Coded Credential Badge (Reference 14-1) in front of the proximity reader. The A2 Emergency Work Designation Code permits MAA SAP entry, as specified in 18.1.2.1.1.a. The security officer ensures only one individual enters the MAA SAP at a time, but does not enforce the one-man occupancy rule during admittance functions or conduct the contraband search. Positive personnel identification is established in accordance with 18.1.2.1.1.b. Entry to the vault is as specified in 18.1.2.1.1.a of this plan.

Fire

The nature of a fire, coupled with the potential malfunction of entry control components and the necessity for a personnel evacuation, places an extreme burden on personnel entry controls and MAA SAP operations. Whenever possible, the MAA SAP is utilized to assemble personnel responding to an A1 emergency. Should the fire make MAA SAP occupancy impossible or degrade the performance capabilities of entry control components or procedures, the Vital Area (VA) SAP is utilized as a focal point for consolidating fire response activities.

A1 designated personnel responding to the fire individually request admittance to the MAA SAP by passing their Coded Credential Badge (Reference 14-1) in front of the proximity reader. The A1 Emergency Work Designation Code permits MAA SAP entry, as specified in 18.1.2.1.1.a. The security officer ensures only one individual enters the SAP at a time, but does not enforce the one-man occupancy rule during admittance functions or conduct the contraband search. Positive personnel identification is established in accordance with 18.1.2.1.1.b. Entry controls for MAA-1.1 and VAU-1.1 are designed to accommodate firemen entering the area of a fire. When the Fire Brigade is ready to enter the MAA or the vault, only the first person to enter the controlled area passes his/her Coded Credential Badge (Reference 14-1) in

front of the proximity reader as the CAS or the SAS de-energizes the electronic door strike. Access to the MAA, through MAA-1.1, or the vault, through VAU-1.1, is now unencumbered for the remainder of the Fire Brigade entering the controlled area. Each new entry by the Fire Brigade to the controlled access area occurs in the same manner. In the event entry controls for MAA-1.1 or VAU-1.1 fail, all door locks fail open providing unencumbered access to the controlled area for personnel inside the MAA SAP (MAA for access to the vault).

18.1.2.2.3.b I.D. Verification and Authorization

Entry authorization is verified as specified in 18.1.2.1.1.b for personnel and 18.1.2.1.2.a for material.

Positive personnel identification is verified as specified in 18.1.2.1.1.b.

18.1.2.2.3.c Personnel Escorts

Reference 31-1 describes the procedures and controls for escorting visitors within the MAA and the vault.

18.1.2.2.3.d Contraband Detection

All personnel and materials, except as specified in 18.1.2.2.3.a, are subject to the contraband detecting measures specified in 18.1.2.1.1.d and 18.1.2.1.2.b of this plan.

18.1.2.2.3.e Response to Suspected Unauthorized Personnel

The response to suspected unauthorized personnel is in accordance with 18.1.2.1.1.e and 18.1.2.1.2.c of this plan.

18.1.3 Bypass of Admittance Procedures and Controls

This subsection describes those measures employed to deter, delay, or deny attempts by an adversary, utilizing stealth or force, to bypass admittance procedures and controls. Routine and non-routine admittance measures, identified in 18.1.2.1 and 18.1.2.2, respectively, provide a minimal degree of protection and assurance that attempts to violate entry controls are detected, assessed, and communicated. The following additional measures provide entry control points with the performance capability requirements specified in 10 CFR 73.45 (b).

18.1.3.1 Isolation Capabilities

The MAA SAP is confined within the Vital Area (VA) and is isolated from the MAA by the entry/exit point designated MAA-1.1 and from the Protected Area (PA) by the VA physical barrier (Figure 18-1). The structure is totally enclosed, permitting the passage of personnel and materials through only the MAA SAP and MAA entrance doors. Reference 68-1 describes the MAA SAP in detail.

Personnel desiring access to the MAA are individually admitted to the MAA SAP and contained until the entire admittance operation is satisfactorily completed.

18.1.3.2 Surveillance Capability

During open portal conditions, the MAA SAP is continuously monitored from the CAS and the SAS by CCTV (Reference 11-1). A Microwave Detection System (Reference 57-1) provides continuous surveillance during closed portal operations. In the event a microwave detector annunciates, the MAA SAP is automatically monitored by CCTV from the CAS and the SAS for the purpose of verifying and assessing the alarm.

18.1.3.3 Doors

All doors providing access to the MAA SAP are interlocked to permit only one entry/exit door to be open at a time. Balanced Magnetic Switches (Reference 6-1) alert the CAS and the SAS of each entry and exit event. The security officer inside the MAA SAP also possesses the capability of locking each entry/exit point door while admittance or exiting functions are conducted. This capability ensures the security officer of a one-on-one confrontation with a potential adversary during routine conditions.

Doors, MAA-1.1, MEE-1.1, and VAU-1.1 are bullet resistant and afford a penetration resistance equivalent, as a minimum, to the weakest component of the physical barrier (References 21-1 and 28-1).

18.1.3.4 Entry Control Personnel

Security officers performing entry control functions do not carry a weapon and are monitored by a duress sensor (Reference 22-1) which annunciates in the CAS and the SAS. Only one security officer is present in the MAA SAP at a time performing entry control functions. The second member of the entry control team monitors the MAA SAP remotely by CCTV (Reference 11-1) and can both detect and respond to a bypass attempt.

18.1.3.5 Penetration Resistance

Because the MAA SAP is totally within the confines of the VA (Figure 18-1), it does not possess the physical attributes of the MAA physical barriers. However, the MAA SAP is constructed of materials presenting sufficient penetration resistance to allow the security officer time to ensure MAA-1.1 is closed, should an individual be passing through MAA-1.1 when the bypass attempt is initiated. Reference 68-1 describes the construction of the MAA SAP.

18.1.3.6 Response to a Bypass Attempt

The MAA SAP security officer always attempts to delay and contain the adversary until response personnel arrive at the MAA SAP. The reporting of and the response to an attempt to bypass admittance procedures and controls at an exit/entry control point is in accordance with Chapter 23 of this plan.

18.2 Entry Through Remainder of the MAA/Vault Boundary

This subsection describes those measures employed to deter, delay, or deny attempts by an adversary to penetrate the physical barriers of the MAA or the vault. Physical barriers include walls, floors, ceilings, ventilation ducts (Reference 3-1), and emergency exits (Reference 28-1). Reference 38-1 describes the floor, ceiling, and walls. These protective functions provide assurance that such attempts, utilizing stealth or force, are detected, assessed, and communicated and satisfy the performance capability requirements of 10 CFR 73.45(b).

18.2.1 Detect Boundary Penetration Attempts

The physical barriers of both the MAA and the vault are monitored by components capable of sensing and alerting the CAS and the SAS of an attempted or actual penetration and facilitating assessment of such an occurrence. Table 18-8 identifies each of these components by function and specifies, when appropriate, whether the associated detection capability is primary (P), redundant (R), or diverse (D).

18.2.2 Deter Boundary Penetration Attempts

The physical barriers of the MAA and the vault are fabricated from materials and erected in a manner which provides assurance that penetration attempts by an adversary are deterred. The incorporation of frequent Security Force patrols, warning signs indicating boundary surveillance, adequate lighting, audible alarms, and unobstructed vision provides the perimeter of the physical barriers with an additional deterrence to penetration attempts. Table 18-9 identifies the various measures utilized to provide the MAA and the vault with positive deterrent capabilities.

18.2.3 Response to Penetration Attempts

Security personnel respond to an actual or attempted penetration of a physical barrier in accordance with Chapter 23 of this plan. During the response phase of an actual or suspected penetration attempt, admittance to and all activities within the MAA and the vault are terminated. Normal operations are resumed only after the response force has established control of the penetration attempt or a surveillance component malfunction has been verified.

TABLE 18-1

WORK DESIGNATION CODES IDENTIFYING
CATEGORIES OF ACTIVITIES INDIVIDUALS MAY BE
AUTHORIZED TO PERFORM WITHIN A MAA OR VAULT

Work Designation Codes	Categories of Work
A. AGNS Employees	
LP	Licensee Personnel
LP-1	Operations
LP-2	Maintenance
LP-3	Security
LP-4	Escort
LP-5	Management
LP-6	Administration
LP-7	Janitorial
LP-8	Health Physics
LP-9	Safety
LP-10	QA/QC
LP-11	Nuclear Technology
B. Visitors	
SLP	State and Local Personnel
SLP-1	LLEA
SLP-2	Fire
SLP-3	Governmental
FO	Federal Officials
FO-1	NRC Inspectors
FO-2	Other NRC Personnel
FO-3	IAEA
FO-4	Other Governmental
V-1	All Others

TABLE 18-2

SCHEDULE FOR IDENTIFYING ROUTINE
WORKING AND NONWORKING TIME PERIODS

WORKING PERIODS	SCHEDULE DESIGNATION	
0001 - 0800	Swing Shift	(SS)
0745 - 0815	Shift Change One	(SC-1)
0801 - 1600	Day Shift	(DS)
1545 - 1615	Shift Change Two	(SC-2)
1601 - 2400	Night Shift	(NS)
2345 - 0015	Shift Change Three	(SC-3)

NONWORKING PERIODS	SCHEDULE DESIGNATION	
0001 - 0800	Nonworking Period 1	(NWP-1)
0801 - 1600	Nonworking Period 2	(NWP-2)
1601 - 2400	Nonworking Period 3	(NWP-3)

TABLE 18-3

GENERIC CRITERIA GOVERNING ACCESS AUTHORIZATION
DURING ROUTINE WORKING AND NONWORKING PERIODS

	Working Periods	Working Periods Shift Changes	Nonworking Periods
1. Vaults will be locked.		+	+
2. General maintenance may be performed (excluding access authorization components).	+		
3. Access authorization components may be repaired, adjusted, calibrated or replaced.			+
4. Entry/exit portals will be locked.		+	+
5. Materials may be allowed entry.	+		+*
6. SNM receipt and transfer operations may be performed.	+		
7. Maintenance may not be performed.		+	
8. Access control personnel may not by changed.		+	
9. Emergency exits will be locked to prevent external entrance.	+	+	+
10. No individual may be authorized entry unless escorted by Security Personnel.			+

*Only for access authorization components

TABLE 18-4

METAL DETECTION

OBJECT TO BE SEARCHED	LOCATION			
	Material Access Area Portal Designation MAA-1.1		Vault Portal Designation VAU-1.1	
	Method	Ref	Method	Ref
1. Personnel	Walk Thru	95-1 72-1	N/A	
2. Unsealed Materials				
Clothing	Hand Held	92-1	N/A	
Tools/Metallic Parts	Visual		N/A	
Instrumentation	Sealed*	83-1	N/A	
Cleaning Materials	Hand Held	92-1	N/A	
Boxes/Parcels/Packages	Hand Held	92-1	N/A	
3. Sealed Packages**				

*Tamper indicating seals.

**All sealed packages, except packages sealed with authorized tamper indication seals, are opened prior to entry into the MAA.

TABLE 18-5

EXPLOSIVE DETECTION

OBJECT TO BE SEARCHED	LOCATION			
	Material Access Area Portal Designation MAA-1.1		Vault Portal Designation VAU-1.1	
	Method	Ref	Method	Ref
1. Personnel	Hand Held	33-1	N/A	
2. Unsealed Materials				
Clothing	Hand Held	32-1	N/A	
Tools/Metallic Parts	Hand Held	32-1	N/A	
Instrumentation	Hand Held	32-1	N/A	
Cleaning Materials	Hand Held	32-1	N/A	
Boxes/Parcels/Packages	Hand Held	32-1	N/A	
3. Sealed Packages*	N/A			

*All sealed packages are opened prior to entry into the MAA.

TABLE 18-6

NUCLEAR MATERIAL DETECTION

OBJECT TO BE SEARCHED	LOCATION			
	Material Access Area Portal Designation MAA-1.1		Vault Portal Designation VAU-1.1	
	Method	Ref	Method	Ref
1. Personnel	Hand Held	74-1	N/A	
2. Unsealed Materials				
Clothing	Hand Held	74-1	N/A	
Tools/Metallic Parts	Hand Held	74-1	N/A	
Instrumentation	Hand Held	74-1	N/A	
Cleaning Materials	Hand Held	74-1	N/A	
Boxes/Parcels/Packages	Hand Held	74-1	N/A	
3. Sealed Packages*	N/A	74-1	N/A	

*All sealed packages are opened prior to entry into the MAA.

TABLE 18-7

WORK DESIGNATION CODES IDENTIFYING NONROUTINE RESPONSE ACTIVITIES INDIVIDUALS MAY BE AUTHORIZED TO PERFORM WITHIN A MAA OR VAULT

Work Designation Codes	Response Activities
	A. Emergencies
A1	Fire
A2	Personnel Injury
A3	Explosion
A4	Radiological
A5	Chemical
A6	Bomb Threat
A7	Material Loss
	etc.
	B. Production
B1	Equipment Failure
B2	Equipment Malfunction
B3	Leaks
B4	Stoppages and Blocking
	etc.
	C. Environmental
C1	Lighting
C2	Heating
C3	Air Conditioning
C4	Plumbing
	etc.

TABLE 18-8

COMPONENTS UTILIZED FOR SENSING, TRANSMITTING, AND ASSESSING PHYSICAL BARRIER PENETRATION ATTEMPTS

SENSING

Area	Type	Reference
MAA	(P) Microwave Systems	57-1
	(D) Video Motion Systems	11-1
Vault	(P) Microwave Systems	57-1
	(D) Video Motion Systems	11-1

TRANSMITTING

Systems	Type	Reference
Microwave	(P) Individual Hardwire	47-1
	(D) Multiplex Hardwire	47-2
Video Motion	(P) Individual Hardwire Video	47-3

ASSESSING

Area	Type	Reference
MAA	(P) CCTV Surveillance	10-1
	(D) Patrols	43-1
Vault	(P) CCTV Surveillance	10-1
	(D) Patrols	43-1

TABLE 18-9

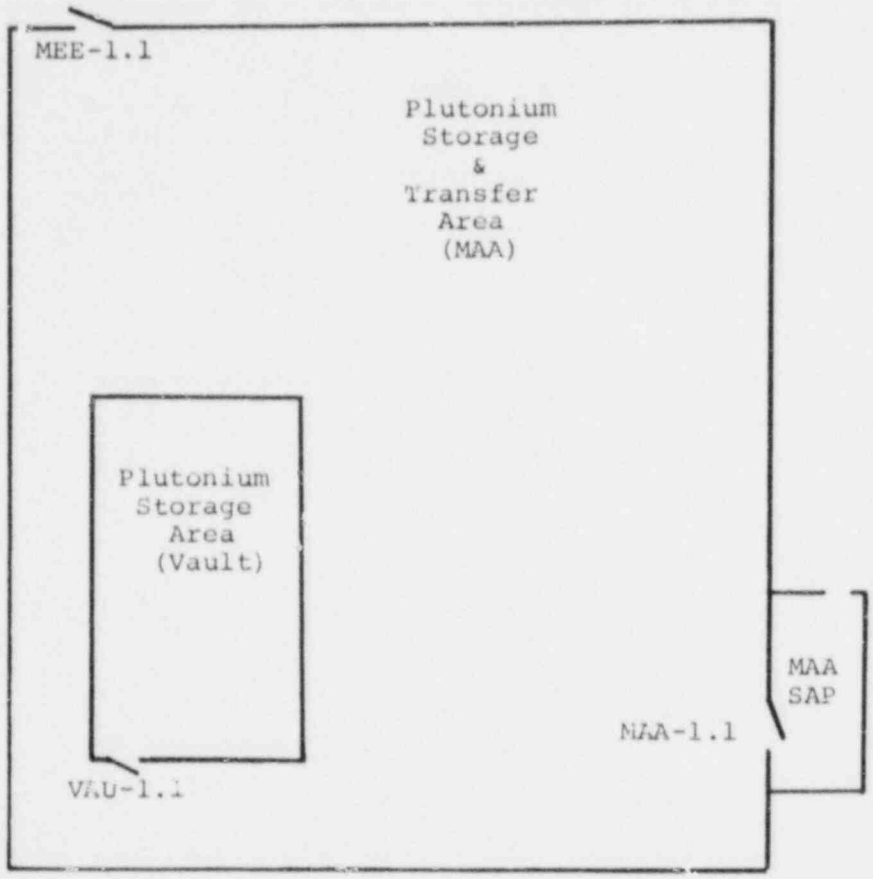
MEASURES UTILIZED TO DETER ADVERSARY PENETRATION ATTEMPTS

Area	Type of Measure	Reference
MAA	Barriers (Walls)	38-1
	Patrols	43-1
	Signs	*
	Lighting	17-1
	Alarms (Microwave)	51-1
	(Video Motion)	11-1
Vault	Barriers (Walls)	38-1
	Signs	*
	Lighting	17-1
	Alarms (Microwave)	51-1
	(Video Motion)	11-1

*No Information Request Sheet identified

FIGURE 18-1

MAA AND VAULT BLOCK DIAGRAM



Plutonium Processing Area
(Vital Area)

4.0 INFORMATION REQUEST SHEETS

Information Request Sheets (IRS) provide detailed technical information supporting the rationale for selection and utilization of a procedure, component, or system in the Physical Protection System. This information is necessary in evaluating the plan's ability to comply with the performance capability requirements of the Physical Protection Upgrade Rule.

Additionally, each IRS is evaluated by an Effectiveness Test Questionnaire (ETQ). The ETQ's utilize the same referencing system as the IRS forms, therefore, associated IRS and ETQ forms possess the same reference numbers. Section 5.0 discusses the purpose of and contains the ETQ answer sheets.

ADMITTANCE AUTHORIZATION CRITERIA AND SCHEDULES

I. FUNCTION

Admittance authorization criteria and schedules are developed for the purpose of determining WHAT activities are authorized, WHO is authorized to perform these activities, and WHEN these activities are authorized to be performed.

II. SYSTEM DESCRIPTION

Admittance authorization criteria and schedules are incorporated into a computerized admittance criteria screening process. This screening process, initiated by the Access Control System (Reference 14-1), integrates data stored in two authorization files: the Personnel Authorization File (PAF) and the Area Authorization File (AAF). The PAF contains the admittance authorization criteria possessed by each employee and preprocessed visitor. The AAF contains the admittance authorization criteria requirements for admittance into each controlled access area within the Industrial Security Area (ISA).

The integration of data contained in the PAF and the AAF results in admittance authorization verification (Reference 2-1).

III. PERFORMANCE CRITERIA

A. Performance Conditions for Personnel

1. Personnel Authorization File (PAF)

a. Personal Authorization Criteria

The following record of admittance authorization criteria is maintained in the PAF for all employees and preprocessed visitors:

(1) Qualification Criteria

(a) Employee or visitor

(b) Basic radiation safety training (YES or NO)

(c) Advanced radiation safety training (YES or NO)

(d) Security clearance (AGNS, DOE Q or L, NRC Q or L)

(e) Work Designation Codes (Table 18-1)

(f) Emergency Work Designation Codes (Table 18-7).

(2) Work Period Criteria

Work period criteria identifies those shifts for which the individual is authorized to be on-site (Table 18-2). Work period criteria is determined by the Shift Schedule which is derived from a detailed analysis of the facility's operational and support requirements.

b. Entering Personal Authorization Criteria

To prevent collusion by individuals authorized to enter personal admittance authorization criteria into the PAF, no two individuals are capable of programming the PAF with sufficient information to authorize an individual admittance into a controlled access area. The following indicates responsibilities for entering personal authorization criteria into the PAF:

(1) Employee/Visitor - Personnel Manager

(2) Basic Radiation Safety Training - Training Manager

(3) Advanced Radiation Safety Training - Health Physics Supervisor

(4) Security Clearance - Security Manager

(5) Work Designation Codes - Personnel Manager

(6) Emergency Work Designation Codes - Site Emergency Director

(7) Work Period Criteria - Physical Security Supervisor.

2. Area Authorization File (AAF)

a. Area Authorization Criteria

The following record of admittance authorization criteria requirements is maintained for all controlled access areas within the ISA:

(1) Baseline Criteria

(a) Employee or Visitor

(b) Completed Basic Radiation Safety Training

(c) Completed Advanced Radiation Safety Training

(d) Security Clearance.

(2) Variable Authorization Criteria

Variable authorization criteria determines what activities are authorized and on which shifts these activities are authorized to be performed. Variable authorization criteria are determined by the Production Schedule which is derived from a detailed analysis of the controlled access area's operational and support requirements.

(a) Work Designation Codes (Table 18-1) - Identifies those activities which are authorized for each area.

(b) Work Period Criteria (Table 18-2) - Identifies those periods when the activities are authorized to be performed.

b. Entering Area Authorization Criteria

To prevent collusion by individuals authorized to enter area authorization criteria requirements into the AAF, no two individuals are capable of programming the AAF with sufficient information to allow an individual access to a controlled access area. The following indicates responsibilities for entering area authorization criteria requirements into the AAF:

(1) Employee/Visitor - Physical Security Supervisor

(2) Completed Basic and/or Advanced Radiation Safety Training - Safety and Environmental Control Department Manager

(3) Security Clearance - Security Manager

(4) Work Designation Codes - Plant Manager

(5) Work Period Criteria - Production Superintendent

(6) Emergency Work Designation Codes - Security Shift Supervisor.

NOTE: Emergency Work Designation Codes are only entered into the AAF upon verification of the authenticity of the emergency in accordance with the Contingency Plan and Procedures (Reference 16-1).

B. Performance Conditions for Vehicles

Vehicles are not authorized inside the MAA.

C. Performance Conditions for Materials

Authorization criteria for materials is based upon detailed analysis of the controlled access area's operational and support requirements. A predetermined inventory of frequently required tools, emergency first aid equipment, and materials which are required, but could also be utilized for sabotage, are maintained within the MAA to minimize the introduction of materials through an MAA SAP.

Admittance authorization criteria for materials is in accordance with the Security Work Order (Reference 98-1).

IV. PREPARATION OF SCHEDULES

A. Shift Schedule

The Shift Schedule, prepared on a monthly basis, is a composite of all departmental shift schedules; e.g., operations, security, maintenance, etc. The Physical Security Supervisor is responsible for the preparation of the Shift Schedule. The Security Manager approves the Shift Schedule.

Shift Schedules may be updated by each Security Shift Supervisor, on a daily basis, depending upon operational and support requirements. Any changes to the Shift Schedule are automatically recorded by the control processor. This record, maintained for three years, identifies who made the change and who was affected by the change. Changes to the Shift Schedule are brought to the attention of the Security Manager on the next regularly scheduled working day.

B. Production Schedule

The Production Schedule, prepared on a weekly basis, is a composite of all departmental production schedules. The Production Superintendent is responsible for the preparation of the Production Schedule. The Plant Manager approves the Production Schedule.

The Production Schedule, for routine conditions, may be updated by the Facility Shift Supervisor. During nonroutine conditions (Table 18-7), the Production Schedule may only be updated by the Security Shift Supervisor after verification of the condition in accordance with the Contingency Plan and Procedures (Reference 16-1). Any changes to the Production Schedule are automatically recorded by the control processor. This record, maintained for three years, identifies who made the change. Routine and nonroutine production or environmental changes to the Production Schedule are brought to the attention of the Plant Manager on the next regularly scheduled working day. Emergency (Table 18-7) changes to the Production Schedule are brought to the attention of the Plant Manager in accordance with the Facility Site Emergency Plan.

V. MAINTENANCE OF THE PAF AND THE AAF

The baseline criteria of the AAF and the qualification criteria of the PAF are maintained current by continuous updating by those personnel responsible for entering the data. The variable authorization criteria of the AAF and the work period criteria of the PAF are updated in accordance with IV.A and IV.B, above.

VI. AUDITING

The control processor automatically records any changes to the PAF and the AAF. At least once each month, the QA/QC Department reviews the record of changes to ensure these changes were valid and properly supported by authentic documentation. Documentation includes training records, health physics records, personnel records, and approved shift and production schedules.

VII. VULNERABILITY

Defeating the admittance authorization criteria and schedules requires collusion by at least three individuals. Additionally, these individuals must be extremely knowledgeable about the computer screening process and the data stored in both the PAF and the AAF.

ADMITTANCE AUTHORIZATION VERIFICATION PROCEDURES

I. FUNCTION

Admittance authorization procedures limit controlled access area admittance to only those personnel authorized to perform specifically assigned tasks and at only those times when the performance of these tasks are authorized.

II. SYSTEM DESCRIPTION

The integration of information contained in the Personnel Authorization File (PAF) and the Area Authorization File (AAF), utilizing a computerized admittance criteria screening process, results in admittance authorization verification. See Reference 1-1 for a detailed analysis of the information contained in and the purpose of the PAF and the AAF.

III. PERFORMANCE CRITERIA

A. Performance Conditions for Personnel

1. Employee Admittance

Employee admittance authorization and verification is achieved through the utilization of the Access Control System (Reference 14-1) and, when positive personnel identification is required, the Voice Verification System (Reference 65-1). When positive personnel identification is not a requirement, identification is established utilizing Photo ID Badges (Reference 62-1). This admittance verification and authorization process ensures employees are only admitted to a controlled access area if they have met ALL of the following criteria:

a. Completed the radiation safety training required for access to the controlled access area.

b. Possess the security clearance required for access to the controlled access area.

c. Possess the Work Designation Code or Emergency Work Designation Code corresponding to the type of activities which are presently authorized to be performed within the controlled access area.

d. Authorized to be on-site during this shift.

e. The control processor recognizes the individual as in a controlled access area which borders on the controlled access area for which admittance is desired.

2. Visitor Admittance

a. Visitors - Escort Not Required

Visitors not requiring an escort are identified by a Photo ID Badge (Reference 62-1) with a light-blue background color. These individuals, upon initially reporting to the facility, are processed in a manner identical to facility employees. The Safety and Environmental Control Department Manager may exempt visitors, based upon their professional training, from the radiation safety training admittance authorization criteria. Consequently, admittance authorization and verification is basically the same as that described in III.A.1.

b. Visitors - Escort Required

Visitors requiring an escort are identified by a Photo ID Badge (Reference 62-1) with a red background color. These individuals, upon initially reporting to the facility, are processed in a manner identical to facility employees. This category of visitors is exempt from the radiation training admittance criteria because the safety feature is provided by the escort. Reference 31-1 provides a detailed description of the selection methodologies and functions of an escort. Admittance authorization and verification is essentially the same as that described in III.A.1.

B. Performance Conditions for Vehicles

Vehicles are not permitted inside the MAA.

C. Performance Conditions for Materials

Authorization verification for materials is in accordance with the Security Work Order (SWO) (Reference 98-1).

IV. MAINTENANCE AND TESTING

A. Maintenance

Corrective and preventative maintenance of the components used in the verification process are described in detail in the applicable Information Request Sheet.

B. Testing

At least once per week, admittance to each controlled access area is attempted utilizing an unauthorized individual. This test, performed by Physical Security Officers, verifies the proper operation of the following authorization verification functions:

1. Admittance of an individual not possessing the proper radiation safety training prevented,
2. Admittance of an individual not possessing the proper security clearance prevented,
3. Admittance of an individual not possessing the proper Work Designation Code or Emergency Work Designation Code prevented,
4. Admittance of an individual not authorized to be on-site prevented,
5. Admittance of an individual not identified in a bordering controlled access area prevented.

V. LEVELS OF AUTHORIZATION REQUIRED

		Protected Area	Vital Area	MAA	Vault
A.	Basic Radiation Training	X	X	X	X
B.	Advanced Radiation Training		X	X	X
C.	Security Clearance				
	1. DOE Q			X	X
	2. NRC Q			X	X
	3. AGNS (Various)	X	X	X	X
D.	Work Designation Code	X	X	X	X
E.	Emergency Work Designation Code	X	X	X	X
F.	Work Period Criteria	X	X	X	X

VI. VULNERABILITY

A. The Security Manager verifies the authenticity of all security clearances prior to entering admittance authorization criteria into the Personnel Authorization File (PAF).

B. Defeating the admittance authorization verification system requires collusion by at least three individuals. Additionally, these individuals must be extremely knowledgeable about the Access Control System (Reference 14-1) and the Voice Verification System (Reference 65-1).

AIR AND UTILITY INLET BARRIERS

I. FUNCTION

Air and utility inlet barriers provide a capability for detecting, deterring, and delaying a forced entry into a controlled access area. The delay function facilitates assessment and response activities by Security Officers.

II. SYSTEM DESCRIPTION

The MAA and the vault are provided with numerous types of utility services. The majority of utility services possess inherent characteristics which deter an adversary action, such as steam, electrical, and acid lines. All utility services penetrate the physical barrier of the MAA and vault by passing through sleeves or cable trays. Design criteria limits the size of utility sleeves or trays, excluding ventilation ducting, to a maximum dimension of 12 inches. Any opening which exceeds the design criteria is provided with enhanced security measures.

III. PERFORMANCE CRITERIA

A. Site Conditions

All ventilation ducting enters and exits the MAA and the vault at a minimum distance of 10 feet above the ground or floor level. The minimum distance between openings is limited to twenty-four inches.

B. Performance Conditions

1. Installation

Unused areas of a sleeve or tray are packed with fire-resistance silicon foam.

2. Ventilation Duct Construction

a. Inlet Ducting

Inlet ventilation ducting measures 12" x 26" and is constructed of 20 gauge galvanized steel.

b. Outlet Ducting

Outlet ventilation ducting measures 12" in diameter and is constructed of schedule 10 304L stainless steel.

3. Ventilation Duct Closure Grid Construction

The closure grid enhances the security of the inlet and outlet ventilation ducts. The closure grid is constructed of 1/2-inch steel rods positioned at 6-inch centers.

4. Pentration Times

Barrier	Penetration Equipment	Avg. Time (Minutes)
Grid	Explosives, linear shaped charge (0.3 lbs.), sledge, chisel, rope	1.0
Grid	Cutting torch, oxy-lance, self contained breathing apparatus	3.3
Vent Duct	Sledge, axe, tin snips, chisel, rope	1.5*

*This time is approximate. The elevated position of the ventilation ducting and the required spacing between sleeves or trays reduces the desirability of such attempts and slightly increases the penetration time.

IV. DETECTION AND ASSESSMENT

A. Detection

1. Security officers observe the VA side of all MAA physical barriers penetrated by the ventilation ducting at least once every 30 minutes. Reference 43-1 discusses patrolling by guard force.

2. During closed portal conditions, a microwave motion detection system (Reference 57-1) monitors the area through which the ventilation ducting penetrates the MAA and vault side of the physical barrier. Sensors annunciate locally and remotely with audible and visual indications. The remote alarm is communicated to the CAS and the SAS.

3. During open portal conditions, CCTV (Reference 10-1) monitors the area through which the ventilation ducting penetrates the physical barrier of both the MAA and vault. During closed portal conditions, the CCTV monitors only the VA side of the MAA's physical barrier.

B. Assessment

An alarm condition is assessed by the security officers patrolling the VA and remotely by CCTV (Reference 10-1) from the CAS and the SAS.

V. ALARM TESTING

A. Microwave Detection System

See Reference 57-1 for testing modes and frequencies.

B. CCTV

See Reference 11-1 for testing modes and frequencies.

VI. VULNERABILITY

A. Ventilation ducts do not contain any features which degrade the penetration times identified in III.B.3 above.

B. The utilization of thermal equipment within the Vital Area is strictly controlled by Security Work Orders (Reference 98-1). Resultantly, this type of penetration equipment is not considered in the determination of penetration delay times. An outside adversary's penetration time is substantially increased when the equipment is transported to the MAA from outside the VA.

BALANCED MAGNETIC SWITCHES

I. FUNCTION

Balanced magnetic switches detect the opening of doors comprising part of the MAA and the vault physical barrier. They also provide remote indication of the return of these doors to a secure status upon completion of the entry or exit operation.

II. SYSTEM DESCRIPTION

The Kiddle, Model DR-850, Balanced Magnetic Switch utilizes a magnetic assembly containing an adjustable permanent magnet and a switch assembly. The switch assembly contains two magnetic reed switches for break and cross actuation.

III. PERFORMANCE CRITERIA

A. Site Conditions

1. MAA-1.1, MEE-1.1, and VAU-1.1 are each equipped with one balanced magnetic switch.

2. The switch assembly is housed within the frame of the door. The adjustable permanent magnet is mounted on the door adjacent to the switch assembly. When the door is closed, neither the switch assembly nor the permanent magnet is exposed.

B. Environmental Conditions

The balanced magnetic switch is designed for both exterior and interior use. Additionally, the MAA and the vault do not contain any normally occurring environmental conditions which adversely affect the performance of the magnetic switch.

C. Performance Conditions

1. System Operation

A magnetic field, generated by the door being in the "secure" position, maintains the switch assembly in a neutral position. Any change in the strength of the magnetic field, caused by the movement of the permanent magnet or the introduction of a foreign magnetic field, results in a loss of balance and the annunciation of the alarm.

2. Installation

Wire-runs are placed in conduit. The conduit is located within the confines of the physical barrier and is not exposed to personnel. Extra wires are included to accommodate the installation of additional sensors and to minimize future maintenance problems.

3. Door Construction

Doors are constructed from nonferrous materials. Each door has a maximum of two millimeters of free play.

Specific Construction Criteria

Door	Reference
MAA-1.1	21-1
MEE-1.1	28-1
VAU-1.1	21-1

4. Reliability

Balanced magnetic switches rarely false alarm and are considered an extremely dependable intrusion detector.

5. Protective Features

a. Tamper protection is an inherent quality of the balanced magnetic switch. Any increase or decrease in the strength of the magnetic field initiates an alarm.

b. Line supervision is not provided. However, to open the door, the locking mechanisms must be de-energized. This action also initiates an alarm.

IV. MAINTENANCE AND TESTING

A. Maintenance

All maintenance is performed by technical security officers.

1. Corrective Maintenance

Corrective maintenance is performed on an as-needed basis.

2. Preventative Maintenance

Preventative maintenance is performed at least once every six months.

B. Testing

All testing is performed by physical security officers.

1. Emergency Exits

Emergency exits are tested once per shift by opening the door and verifying the proper operation of the magnetic switch and associated alarms.

2. Entry/Exit Doors

Entry/exit doors are tested once per shift by opening the door and verifying the proper operation of the magnetic switch and associated alarms.

V. DETECTION AND ASSESSMENT

A. Detection

The maximum distance the door can be opened without initiating an alarm is one-half inch. This action initiates a local and remote alarm with both audible and visual indication. Reference 51-1 describes in detail the local alarms associated with balanced magnetic switches. Reference 21-1 (Doors and Associated Hardware) and Reference 28-1 (Emergency Exits) identify the location of remote alarms.

B. Assessment

1. Local

Local alarm assessment is conducted by security officers patrolling the area of the alarm. See Reference 43-1.

2. Remote

Remote assessment, via CCTV (Reference 10-1), is conducted from the CAS and the SAS by security officers.

VI VULNERABILITY

A. Balanced magnetic switches only detect opening and closing events. Door penetrations are not detected.

B. Additional detection capabilities are provided by the microwave (Reference 57-1) and video (Reference 11-1) motion detection systems for door opening and closing events and door penetrations.

CCTV MONITORING/SURVEILLANCE

I. FUNCTION

CCTV monitoring/surveillance provides the capability for monitoring activities and conditions inside a controlled access area and for detecting and assessing adversary activities.

II. SYSTEM DESCRIPTION

See Reference 11-1 for a complete description of the CCTV system.

III. PERFORMANCE CRITERIA

A. Performance Conditions

1. Types of Monitors

Operators observe a maximum of two surveillance monitors. For each surveillance monitor, there is an associated spot monitor. All monitors provide a 9-inch diagonal visual display.

a. Surveillance Monitors

Surveillance monitors receive a visual input signal from a maximum of six CCTV cameras. The monitors can be operated in three modes: automatic, manual, and automatic alarm. In the automatic mode, the monitor is connected to the sequencing network which switches the visual display between the input cameras at intervals ranging from 1 to 30 seconds. In the manual mode, the monitor receives an input signal from only one CCTV camera. In the automatic alarm mode, the monitor is sequenced and electronically connected to the Video Motion Detection System (VMD) (Reference 11-1) and/or the Microwave Motion Detection System (MMD) (Reference 57-1). When an alarm is initiated, the sequence is interrupted and the monitor produces a visual display of the area generating the alarm. Additionally, if more than one alarm is received, the sequencing network switches between only the VMD cameras and/or the MMD units transmitting the alarm signal.

b. Spot Monitors

Spot monitors allow the operator to continuously view an area of concern or one in which

an alarm has been initiated. Spot monitors can also be operated in three modes which are identical to surveillance monitors.

2. Monitor Placement

Monitors are positioned on the vertical portion of the display console at eye level.

3. Observation Periods

a. Observing Periods

The maximum observing period does not exceed two hours.

b. Recovery Periods

For every two hours of observing, the operator receives one hour of recovery time. This ratio of 2:1 is maintained for any length of observing period.

4. Controls

Operator controls are located horizontally on the console within reach of the operator and directly below the monitors such that control manipulation does not obstruct the visual path of the operator. Controls and switches, including those for the sequencing network, the video recorder, the VMD system, and the MMD system, are grouped together and arranged in direct relationship to the monitors they control.

5. Diversity and Redundancy

a. When a surveillance monitor becomes inoperative, the spot monitor becomes the surveillance monitor. Spare monitors are immediately available to minimize the downtime of CCTV monitoring capabilities.

b. In the event environmental conditions prevent visual surveillance by CCTV monitors, the controlled access area is continuously patrolled by security officers (Reference 43-1) and manned by security response personnel.

6. Operator Training

Security officers receive classroom and on-the-job training prior to being authorized to operate CCTV monitors and to perform surveillance and assessment functions. This training, utilizing written procedures where applicable, includes instructions for properly operating the CCTV monitors, proper assessment techniques, and proper response procedures.

IV. MAINTENANCE AND TESTING

A. Maintenance

See Reference 11-1.

B. Testing

Operators are randomly tested on a weekly basis to determine their surveillance and assessment capabilities and to motivate operators to maintain vigilance while observing CCTV monitors.

V. DETECTION AND ASSESSMENT

See Reference 11-1.

VI. VULNERABILITIES

See Reference 11-1.

CCTV SYSTEMS

I. FUNCTION

CCTV systems provide the remote capability for continuous monitoring, sensing, detecting, and assessing adversary activities within a controlled access area.

II. SYSTEM DESCRIPTION

The Venus Scientific, Model DV-1, Low Light CCTV system is employed. The system incorporates an all solid state, intensified Vidicon TV camera which utilizes a 25-millimeter image intensifier with a 1-inch Vidicon tube. The system is capable of operating within a light range varying from bright sun light to 5.0 E-05 foot candles, face plate illumination.

III. PERFORMANCE CRITERIA

A. Site Conditions

1. CCTV cameras are positioned within the area of coverage such that blind spots are eliminated.

2. For spaces having a height of 20 feet or less, CCTV cameras are normally positioned at a height varying from 12 to 14 feet. A minimum height of 9 feet is always maintained, unless lower levels are specifically required. For spaces having a height of 21 feet or greater, CCTV cameras are positioned to provide multiple viewing levels.

B. Environmental Conditions

1. Man-made

   a. Man-made environmental conditions are all controlled such that they do not adversely affect the proper operation of the CCTV system.

   b. Cameras and transmission lines, by design, are immune to EMI under normal conditions. Additional EMI protection is provided by restricting RF radiating equipment to only the security officers' duress alarm systems (Reference 22-1).

2. Natural

The Vital Area (VA), MAA SAP, MAA, and vault are each located inside the facility. Resultantly, natural phenomenon is not expected to adversely affect the proper operation of the CCTV systems. Lightning protection is provided by facility design considerations and power line filtering.

C. Performance Conditions

1. Operation

a. Closed Portal Conditions

Each CCTV camera is associated with a Microwave Motion Detection unit. When the microwave unit (Reference 57-1) detects motion within its area of coverage, the CCTV camera is automatically activated.

b. Open Portal Conditions

During open portal conditions, all cameras are operative. An automated switching network presents the area of coverage to the monitor in a timely and useful manner. The monitor has the capability to selecting any of the cameras, should he be interested in viewing a specific area for a period of time longer than presented by the switching network. Additionally, CCTV systems are provided with a Video Motion Detection system. This system allows the monitor to segregate the total area of coverage into a free access area and a restricted access area by masking the free access areas.

2. Lighting System

To ensure adequate lighting for the CCTV systems, controlled security lighting maintains a minimum illumination level of 5.0 E-03 foot candles, face plate illumination, during all conditions. Planned lighting ensures even illumination over the area of coverage and minimizes glare and bright spots. See Reference 17-1 for a complete description of the controlled security lighting system.

3. Switching Network

Switching is accomplished by the Panasonic Auto Alarming Sequential Switcher, Model WJ-510A. Roll free video switching for the cameras utilizes an external, master synchronization system. The security officer monitoring the cameras has the capability of interrupting the video switching sequence at any time.

4. Video Recording

Alarm video is routed to a Panasonic Time Lapse Video Recorder, Model NV-8030. Upon receipt of an alarm condition from the microwave detection unit (Reference 57-1) or the Video Motion Detection system, the switcher routes the signal to the recorder. The recorder then changes from one of four available slow speeds (9, 18, 72, and 108 hours) to high speed to record activities within the area of coverage. Recording time speeds can be controlled from the and SAS or by programming the recorder.

5. Elimination of Nuisance Alarms

Because the controlled access areas are inside the facility, nuisance alarms from external factors are not expected to be significant. Also, the Video Motion Detection system is provided with the capability of masking areas not subject to coverage to prevent false alarms.

6. Target Visibility

Target visibility is accomplished by thorough illumination planning and fixture placement in the controlled access area. Reference 17-1 describes the controlled security lighting system design criteria.

7. System Resolution

CCTV systems are capable of distinguishing a man's face at any point within the area of coverage under both normal and emergency lighting conditions.

8. Power Supplies

CCTV systems are provided with both UPS (Reference 85-1) and Emergency Generating Systems (EGS) (Reference 29-1) as backup power supplies. Upon a loss of normal electrical power, CCTV systems automatically switch to the UPS within 1/60 of a second. Once the EGS is prepared to assume the full load, approximately 15 seconds, CCTV systems automatically switch to the EGS, also within 1/60 of a second. UPS can carry all critical loads for a period of one hour. The EGS can carry all critical loads for a period of 30 days.

9. Video Motion Detection System (VMD)

The VMD system is capable of detecting motion by dividing the restricted access area (unmasked) of the video display into segments. Each segment is divided into 10 shades of the RETMA gray scale and assigned digital numbers from one to ten which correspond to specific shades of gray. If any of the values change due to motion within the area, by more than a value of two, an alarm is registered.

10. Diversity and Redundancy

a. Closed Portal Conditions

During closed portal conditions, the Video Motion Detection system is backed up by the Microwave Motion Detection System (Reference 57-1).

b. Open Portal Conditions

Cameras are mounted in pairs such that the area of coverage is overlapped. Additionally, all camera positions are monitored by other CCTV cameras.

IV. DETECTION AND ASSESSMENT

A. Detection

1. The Microwave Detection System (Reference 57-1) annunciates audibly and visually, both remotely and locally. Remote alarm annunciation is in the CAS and the SAS.

2. The Video Motion Detection System annunciates, both visually and audibly in the CAS and the SAS.

3. Detection of adversary actions is also accomplished by the monitor viewing the visual display, either in the remote monitoring station (CAS and SAS) or the MAA SAP.

B. Assessment

1. Remote Assessment

An alarm condition or potential adversary action is assessed by CCTV from the CAS and the SAS.

2. Local Assessment

Local assessment is performed by security officers patrolling the VA and response force personnel. Additionally, the security officer inside the MAA SAP has the capability to assess potential adversary action outside the MAA SAP via CCTV.

V. MAINTENANCE AND TESTING

A. Maintenance

1. Corrective Maintenance

Corrective maintenance is performed on an as-needed basis. Spare parts and components are maintained in supply to minimize the downtime of a CCTV system.

2. Preventative Maintenance

Preventative maintenance is performed in accordance with a mean-time-between failure schedule. For all equipment, except the video recorder, maintenance is semiannual. For the video recorder, inspections, and adjustments are performed at specific hours of operation, such as every 250, 500, and 1,000 hours.

B. Testing

All video systems are tested 30 minutes prior to the day shift (DS) (see Table 18-2). These tests include ensuring adequate monitoring capabilities from the CAS and SAS and the presence of proper lighting and power requirements.

VI. VULNERABILITIES

A. All critical components are located within controlled access areas.

B. Tamper protection is accomplished by physical placement of the cameras and a signal supervising system.

1. Physical Tamper Protection

Each TV camera is monitored by another TV camera during open portal conditions. During closed portal conditions, a microwave unit protects the integrity of each TV camera.

2. Signal Supervising

A signal supervising system monitors the output of each camera. If the signal is interrupted for more than 0.1 millisecond, a tamper warning is initiated.

CODED CREDENTIAL SYSTEMS

I. FUNCTION

The coded credential system is utilized to verify admittance authorization to controlled access areas.

II. SYSTEM DESCRIPTION

The Schlage, Model 414, Access Control System employs a standard credit card size passive-electronic-coded credential badge and a proximity reader. The credential badge contains a laminated, electronically tuned circuit which responds to three specific RF frequencies in the range of 4 to 30 MHz. The Schlage Access Control System has a maximum capacity of 1,500 credential badges and can control up to eight (custom systems can accommodate more) proximity readers located a maximum distance of 305 meters from the system's control processor.

III. PERFORMANCE CRITERIA

A. Performance Conditions

1. Operation

a. Issuing

An individual desiring access to the Industrial Security Area enters a personnel portal located at the Main Gate and is issued a coded credential badge. Within the personnel portal, the individual positions the coded credential badge on the Schlage proximity reader and enters his employee number on the control processor's communications terminal. This action inputs the Voice Verification System (VVS) (Reference 65-1) which requests the individual to repeat a randomly selected sequence of four prerecorded words. A satisfactory response inputs the VVS to signal the control processor to identify the coded credential badge identification number with the employee identification number for all subsequent admittance requests.

b. Obtaining Access to Controlled Areas

To obtain access to a controlled access area, the person positions the coded credential badge within 10 centimeters of the proximity reader

located next to the entrance door. The credential's identification number is read and transferred to the control processor which, after associating the credential's identification number with the individual's employee number, scans the PAF and the AAF to determine if access is authorized. Access authorization inputs the control processor to initiate admittance operations to the area for which admittance has been requested.

c. Badge Retention

All personnel exiting the Industrial Security Area return their coded credential badges to the Main Gate security officer. Credential badge identification numbers are removed from the control processor's memory at the end of each shift.

2. Protective Features

a. Anti-Pass-Back

Once a coded credential badge is utilized to gain access to an area, the control processor only allows the coded credential badge to be used to exit the area or to enter the next elevated security area within the controlled access area. Any attempt to use the coded credential badge in another manner, such as to request admittance to the same controlled access area, is rejected by the control processor.

b. Lost or Stolen Badges

Each coded credential badge contains a unique identification number. In the event a credential badge is lost or stolen, the control processor is programmed to reject any future use of the badge for controlled area admittance.

3. System Interfaces

a. Positive Personnel Identification

Admittance to a MAA requires positive personnel identification. When a coded credential badge is utilized to gain admittance to a MAA's SAP, the control processor automatically inputs the

VVS with the employee number of the individual. Once inside the MAA SAP, the VVS requests the individual to repeat a randomly selected sequence of four prerecorded words. A satisfactory response inputs the VVS to signal the control processor that positive personnel identification has been established.

b. Personnel Inventory System

Each entry and exit operation using a coded credential badge inputs the control processor to upgrade the occupancy listing for each controlled access area within the Industrial Security Area. Security officers have the capability of displaying a listing of all personnel occupying a specific controlled access area and to tract personnel throughout the facility and determine their present location.

4. Accountability

The Security Department is responsible for ordering, receiving, auditing, conducting inventories, issuing, decoding, and destroying all credential badges.

IV. SYSTEM VULNERABILITY

a. The passive-electronic-coded credential badge system ranks as one of the two most difficult of all coded credential systems to duplicate or decode. Additionally, badges are randomly issued each time an individual enters the Industrial Security Area. This procedure eliminates the threat of duplication because one never knows which coded credential badge he will be issued.

b. The Schlage Access Control System does not possess the capability to detect equipment tampering. However, the proximity readers may be installed inside a wall, thus eliminating exposed parts. Additionally, the coded credential badge does not contain access authorization information, it is only the instrument by which the control processor identifies the individual requesting admittance. All access information is contained in the PAF and the AAF.

CONTROLLED SECURITY LIGHTING

I. FUNCTION

Controlled security lighting for the MAA, the MAA Secured Access Portal (SAP), and the vault provides illuminiation for monitoring, surveillance, and alarm assessment.

II. SYSTEM DESCRIPTION

Controlled security lighting for the MAA and the vault is provided by incandescent lighting. All of the lighting in the MAA SAP, including controlled security lighting, is provided by incandescent lights.

III. PERFORMANCE CRITERIA

A. Environmental Conditions

The MAA, vault, and MAA SAP are each located inside the facility. Environmental conditions are not expected to adversely affect the proper operation of the controlled security lighting system. Lightning protection is provided by the facility housing the controlled access areas.

B. Performance Conditions

1. Illumination Design Criteria

Monitoring, surveillance, and alarm assessment inside the MAA, MAA SAP, and the vault is primarily conducted utilizing CCTV (Reference 10-1). Resultantly, the following criteria defines the illumination standards to which the controlled security lighting system is designed:

a. Minimum illumination is a function of the sensitivity and spectral response of the video image tube, the aperature and light transmission of the lens, and the area reflectivity. See Reference 11-1 for the specific characteristics of the CCTV system employed. Minimum illumination is set at 5.0 E-03 foot candles.

b. Maximum illumination within the controlled access area minimizes CCTV picture washout. The max/min illumination ratio is less than 10.

c. Light sources and CCTV cameras are positioned to minimize glare and bright spots.

d. Illumination over the entire viewing area provides well-defined images on the CCTV monitor.

2. Reliability

The integrity of the controlled security lighting system is maintained by the integration of the following systems to ensure sufficient lighting is maintained with the MAA, MAA SAP, and the vault at all times.

a. Multiple Lighting Circuits

The controlled security lighting system is composed of two lighting subsystems which are supplied with electrical power through separate distribution circuits. A loss of power to or a failure of one circuit does not prevent the controlled security lighting system from satisfying the illumination standards described in III.B.1 above.

b. UPS (Security Lighting)

Both controlled security lighting subsystems are protected by a Security UPS (Reference 85-1). The transfer of electrical power is automatic and instantaneous. The security UPS can sustain the controlled security lighting system for a period of one hour.

c. Emergency Generating System (EGS)

Both controlled security lighting subsystems are also connected to the EGS (Reference 29-1). In the event of a loss of normal electrical power, the EGS assumes the full electrical load of all UPS systems and other designated loads within 12 to 15 seconds of the loss of power and can sustain these loads for a period of 30 days.

IV. MAINTENANCE AND TESTING

A. Maintenance

All controlled security lighting maintenance is performed by authorized maintenance personnel and witnessed by Technical Security Officers.

1. Corrective Maintenance

Corrective maintenance is performed on an as-needed basis. Spare lighting and circuitry components are maintained in supply to minimize the down-time of a controlled security lighting subsystem.

2. Preventative Maintenance

Preventative maintenance is performed in accordance with a Mean-Time-Between-Failure (MTBF) schedule. For the majority of controlled security lighting components, preventative maintenance is performed on a semiannual basis.

B. Testing

The controlled security lighting system is continuously checked by security officers patrolling the controlled access areas (see Reference 43-1). Illumination levels are verified on a bi-weekly basis in all controlled access areas by Physical Security Officers.

V. VULNERABILITIES

A. All of the controlled security lighting components (lamps, control panels, etc.) are located inside the MAA. Junction boxes, cable runs, and the UPS and EGS systems are located within a Vital Area (VA).

B. Controlled security lighting is monitored continuously by tamper indicating circuitry.

ENTRY/EXIT DOORS

I. FUNCTION

Entry/exit doors provide access control and a capability for detecting, deterring, and delaying a forced entry into a controlled access area. The delay function facilitates assessment and response activities by Security Officers.

II. SYSTEM DESCRIPTION

MAA-1.1 and VAU-1.1 are personnel doors comprising part of the physical barrier for the MAA and the vault, respectively (see Figure 18.1). MAA-1.1 is located on an inside wall. Both doors are custom manufactured and provide a high degree os security.

III. PERFORMANCE CRITERIA

A. Performance Conditions

1. Door and Frame Construction

a. Door

Doors are constructed of 3/4-inch (outside) steel plate, a 3-inch block of redwood, and a 1/2-inch (inside) steel plate. The redwood is anchored to both steel plates with stud nails placed at 6-inch intervals.

b. Frame

Frames are constructed of steel and possess penetration resistance times equivalent to that of the entry/exit doors. A 1/2-inch steel lip, welded to the outside of the door, conceals the opening between the door and the frame.

2. Door and Frame Alignment

Emergency exits have a maximum of 2 millimeters of free play between the door and the frame.

3. Door Hinges

Each door utilizes five hinges located on the inside of the door. The body of the hinge is made of 3/4-inch steel and is welded to both the frame and the door. The hinge pin is made of 3/4-inch steel and is not exposed. Hinge pins are welded to

the hinge body attached to the frame. Door hinges allow opening the door only in the outward direction.

4. Door Locking Mechanisms

a. Description

Two active dead bolt systems per door are employed. The active dead bolts, each a 1-1/2-inch diameter stainless steel rod, and the actuators are positioned inside the wall. The length of the dead bolts is randomly selected allowing the actuating mechanisms to be positioned at varying distances from the door. Additionally, the locking mechanisms are randomly placed around the perimeter of the door such that the dead bolts may travel either vertically or horizontally. Dead bolts are spring loaded to return to the "unsecure" position.

b. Operation

In the "secure" position, the actuators are electronically energized and the dead bolts are positioned inside the door. Entry authorization de-energizes the actuator causing the spring to return the dead bolt to the "unsecure" position. Entry/exit doors fail in the "unsecure" position upon a loss of electrical power.

5. Penetration Times

Barrier	Penetration Equipment	Avg. Time (Minutes)
Door	Explosives (9 pounds) tamped charge	1.5*
Dead Bolt	Air/arc welding, high pressure air	6.0**

*1.5 minutes represents the penetration time with a 3-inch void space. An evaluation for redwood has not been conducted.

**Two dead bolts require cutting. Additionally, the 1/2-inch steel lip must be cut and the placement of the dead bolts is varied increasing the penetration time. A more realistic penetration time is approximately 14 minutes.

IV. DETECTION AND ASSESSMENT

A. Detection

1. MAA

The MAA-1.1 opening and closing events are monitored by balanced magnetic switches (Reference 6-1). The alarm annunciates with audible and visual indications both remotely and locally. The remote alarm occurs in the CAS, SAS, and the appropriate MAA SAP.

A line supervising device monitors electrical power supplied to the actuator. The sensor annunciates locally and remotely with audible and visual indications when the actuator is de-energized. The remote alarm is communicated to the CAS, SAS, and the appropriate MAA SAP.

During open portal conditions, the adversary is detected by the Security Officer conducting entry control functions.

During closed portal conditions, the adversary is detected by the microwave motion detection system (Reference 57-1) as he enters the MAA SAP. The sensor annunciates audibly in the MAA SAP and audibly and visually in the CAS and the SAS.

2. Vault

VAU-1.1 opening and closing events are monitored by balanced magnetic switches (Reference 6-1). The alarm annunciates with audible and visual indications both remotely and locally. The remote alarm occurs in the CAS, SAS, and the appropriate MAA SAP.

A line supervising device monitors electrical power supplied to the actuator. The sensor annunciates locally and remotely with audible and visual indications when the actuator is de-energized. The remote alarm is communicated to the CAS, SAS, and the appropriate MAA SAP.

During open portal conditions, the adversary is detected by CCTV (Reference 10-1). The vault entrance is located such that only personnel desiring access to the vault need approach the door. Any such action, when a vault entry is not

scheduled, alerts the Security Officer to a potential adversary action.

During closed portal conditions, the MAA is continuously monitored by a vibration (Reference 87.1) and microwave motion (Reference 57-1) detection system. The sensor annunciates audibly in the MAA and audibly and visually in the CAS and the SAS.

B. Assessment

An alarm condition in the MAA SAP, MAA, or in the vault is assessed by CCTV (Reference 10-1) from the CAS and the SAS.

V. ALARM TESTING

A. Balanced Magnetic Switches

See Reference 6-1 for testing frequencies.

B. Line Supervising Sensor

The sensor is tested once per day by de-energizing the actuator from the CAS or the SAS.

C. Microwave Sensor

See Reference 57-1 for testing frequencies.

VI. VULNERABILITY

A. Entry exit doors do not contain features which degrade the penetration times identified III.A.5, above.

B. The utilization of thermal equipment within the Vital Area is strictly controlled by Security Work Orders (Reference 98-1). Resultantly, this type of penetration equipment is not considered in the determination of penetration delay times. An outside adversary's penetration time is substantially increased when this type of equipment is transported to the MAA.

DURESS ALARMS

I. FUNCTION

Duress alarms detect and communicate those conditions which result in the presence of abnormal physiological responses from a security officer during the performance of his assigned duties.

II. SYSTEM DESCRIPTION

A duress alarm consists of a miniaturized transmitter, a sensor, electrodes, and a battery pack. The sensor monitors changes in the physiological condition, heart beat and galvanic skin conditions, of the security officer via electrodes attached to his chest. These bodily functions increase when an individual is subjected to a threatening situation or decrease in the event of death. Such occurrences, above or below preset limits, trip the sensor and cause the duress alarm to initiate a remote annunciation.

III. PERFORMANCE CRITERIA

A. Siting Conditions

All security officers manning MAA SAP's are monitored by duress alarms. These sensors are concealed under the clothing of the security officer.

B. Environmental Conditions

The environmental conditions of each MAA SAP are controlled such that they do not adversely affect the performance of the duress alarms. Additionally, due to the resistance of the physical barriers of the facility to RF transmissions, RF receivers are installed inside each MAA. The RF receivers are hardwired to the CAS and the SAS to ensure the transmission of alarm signals out of the facility.

C. Performance Conditions

1. Issuing Duress Alarms

Security officers are issued duress alarms prior to assuming responsibility for entry control functions. Once the electrodes are attached, the sensor's alarm limits are adjusted relative to the security officer's present physiolcgical conditions. The sensor is then tested to ensure proper operation.

2. Operation

Each sensor has a preset upper and lower alarm limit. The lower alarm limit provides the capability for detecting the death of the security officer. The upper alarm limit detects elevated heart rate and galvanic skin responses resulting from the occurrence of a stress situation. When either of these limits are reached, the sensor trips and initiates a signal transmission to the CAS and the SAS via the RF receiver.

3. Redundant Features

Security officers are continuously required to interact with the computer processor, via the communications terminal, prior to the individual gaining access to the MAA. When the security officer perceives a threat, he alerts the CAS and the SAS by entering an alert code on the communication terminal.

IV. DETECTION AND ASSESSMENT

A. Detection

Duress alarms annunciate with both audible and visual indications at the CAS and the SAS. A common audible alarm alerts the monitor to the occurrence of a duress alarm. Individual visual displays alert the monitor to the specific location of the duress alarm.

B. Assessment

An alarm condition is assessed by security officers patrolling the area (Reference 43-1) and remotely by CCTV (Reference 10-1) from the CAS and the SAS.

V. MAINTENANCE AND TESTING

A. Maintenance

All maintenance is performed by Technical Security Officers.

1. Corrective Maintenance

Corrective maintenance is performed on an as-needed bases.

2. Preventative Maintenance

Preventative maintenance is performed at least every three months or more frequently when indicated by the manufacturer's maintenance instructions.

B. Testing

Duress alarms are tested, inside the MAA SAP, at the beginning of each shift. The test is conducted by having the security officer run-in-place for one minute and observing the proper operation of the sensor and associated alarm components.

VI. VULNERABILITY

A. The manner in which the security officer perceives the threat, his physical condition, and the training he has received for responding to a stress situation affects the reliability of the duress alarm.

B. Duress alarms are extremely reliable in detecting the death of a security officer.

EMERGENCY EXITS

I. FUNCTION

Emergency exits provide unimpeded egress from a controlled area during an emergency condition. Additionally, emergency exits provide a capability for detecting, deterring, and delaying a forced entry into a controlled access area.

II. SYSTEM DESCRIPTION

MEE-1.1 is an emergency exit (see Figure 18.1) comprising part of the physical barrier for the MAA. The door is located on an inside wall and is equipped with a panic bar mechanism. Emergency exits are custom manufactured and provide a high degree of security. Personnel evacuating from the vault and/or the MAA are channeled into the Vital Area.

VAU-1.1 also serves as an emergency exit and is equipped with a panic bar mechanism for unimpeded egress from the vault. The frequency of vault entries prohibits the installation of a separate vault emergency exit.

III. PERFORMANCE CRITERIA

A. Performance Conditions

1. Door and Frame Construction

a. Door

Doors are constructed of a 3/4-inch (outside) steel plate, a 3-inch block of redwood, and a 1/2-inch (inside) steel plate. The redwood is anchored to both steel plates with stud nails placed at 6-inch intervals.

b. Frame

Frames are constructed of steel and possess penetration resistance times equivalent to that of the emergency exit doors. A 1/2-inch steel lip, welded to the outside of the door, conceals the opening between the door and the frame.

2. Door and Frame Alignment

Emergency exits have a maximum of 2 millimeters of free play between the door and the frame.

3. Door Hinges

Each door utilizes five hinges located on the inside of the door. The body of the hinge is made of 3/4-inch steel and is welded to both the frame and the door. The hinge pin is made of 3/4-inch steel and is not exposed. Hinge pins are welded to the hinge body attached to the frame. Door hinges allow opening the door only in the outward direction.

4. Door Locking Mechanisms

a. Description

Two active dead bolt systems per door are employed. The active dead bolts, each a 1-1/2-inch diameter stainless steel rod, and the actuating devices are positioned inside the wall. The length of the dead bolts is randomly selected allowing the actuator to be positioned at varying distances from the door. Additionally, the locking mechanisms are randomly placed around the perimeter of the door such that the dead bolts may travel either vertically or horizontally. Dead bolts are spring loaded to return to the "unsecure" position.

b. Operation

In the "secure" position, the actuators are electronically energized and the dead bolts are positioned inside the door. Operating the panic bar de-energizes the actuator. This action causes the spring to return the dead bolt to the "unsecure" position allowing unimpeded egress from the door. Emergency exits fail in the "unsecure" position upon a loss of electrical power.

5. Penetration Times

Barrier	Penetration Equipment	Avg. Time (Minutes)
Door	Explosives (9 pounds) tamped charge	1.5*
Dead Bolt	Air/arc welding, high pressure air	6.0**

IV. DETECTION AND ASSESSMENT

A. Detection

1. Emergency exit opening and closing vents are monitored by balanced magnetic switches (Reference 6-1). The alarm annunciates with audible and visual indications both remotely and locally. The remote alarm occurs in the CAS, SAS, and the appropriate MAA SAP.

2. A line supervising device monitors electrical power supplied to the actuator. The sensor annunciates locally and remotely with audible and visual indications when the actuator is de-energized. The remote alarm is communicated to the CAS, SAS, and the appropriate MAA SAP.

3. The outside area of each emergency exit is monitored by CCTV (Reference 10-1) continuously. During open portal conditions, the emergency exit area inside the MAA is continuously monitored.

4. A microwave motion detection system (Reference 57-1) monitors the emergency exit area inside the MAA during closed portal conditions. The sensor annunciates locally and remotely with audible and visual indications. The remote alarm is communicated to the CAS and the SAS.

---

*1.5 minutes represent the penetration time with a 3-inch void space. Evaluations using redwood have not been conducted.

**Two dead bolts require cutting. Additionally, the 1/2-inch steel lip must be cut and the exact placement of the dead bolts is varied increasing the penetration time. A more realistic penetration time is approximately 14 minutes.

5. Security Officers routinely, but in a randomly selected order, patrol emergency exits leading into the Vital Area. Security Officers observe each emergency exit at least once every 30 minutes. Reference 43-1 discusses patrolling by the guard force.

B. Assessment

An alarm condition is assessed by Security Officers patrolling the area and remotely by CCTV (Reference 10-1) from the CAS and the SAS.

V. ALARM TESTING

The balanced magnetic switches and the line supervising sensor are tested once per shift by Security Officers. This test is conducted by operating the panic bar and opening the emergency exit. The microwave detection system is tested once per week by opening MAA-1.1 while the system is in operation.

VI. VULNERABILITY

A. Emergency exits contain no features which degrade the penetration times identified in III.A.5., above.

B. The utilization of thermal equipment within the Vital Area is strictly controlled by Security Work Orders (Reference 98-1). Resultantly, this type of penetration equipment is not considered in the determination of penetration delay times. An outside adversary's penetration time is substantially increased when this type of equipment is transported to the MAA.

EQUIPMENT CHECKS/MAINTENANCE

I. FUNCTION

The equipment checks and maintenance procedure provide a means of ensuring the operational condition of and documenting the maintenance history of all physical protection components.

II. SYSTEM DESCRIPTION

A maintenance history record is maintained for each physical protection component. The record is maintained for the life of the component or five years whichever is greater. These records contain the following data for each maintenance action performed on the component:

A. Date of the equipment check/maintenance.

B. Symptoms initiating the maintenance action. If the maintenance was performed in accordance with a Mean-Time-Between-Failure (MTBF) schedule, identify the MTBF preventative maintenance identification number.

C. Maintenance performed, adjustments made, modifications completed, parts replaced, etc.

D. Signatures of the personnel conducting the maintenance, the close-out inspection, and the operational tests.

E. Documentation of parameters measured, when appropriate.

F. Any supporting information.

III. PERFORMANCE CRITERIA

A. Performance Conditions

1. Scheduling Equipment Checks/Maintenance

a. Corrective Maintenance

Corrective maintenance is performed during non-routine conditions. Consequently, scheduling of corrective maintenance cannot be scheduled in advance.

b. Preventative Maintenance

All preventative maintenance on physical protection systems and systems which interface the physical protection components is performed in accordance with work schedules approved by the Plant Manager and the Production Superintendent (Reference 1-1, III.2.b). A weekly production schedule is distributed to all departments identifying those activities which are authorized and when these activities are authorized to be performed.

2. Performing Equipment Checks/Maintenance

a. Physical Protection Components

All maintenance is performed by two equally knowledgeable Technical Security Officers. Upon completion of the work, a knowledgeable third person, also a Technical Security Officer, performs a close-out inspection. All personnel are then required to complete the maintenance history record.

b. Interfacing Components

Maintenance performed on nonsecurity components which interface with physical protection components, such as the Emergency Generating System, is conducted by facility maintenance personnel. All such maintenance is witnessed by a competent Technical Security Officer. Upon completion of the work, a third person from the maintenance group and the Technical Security Officer witnessing the maintenance performs a close-out inspection. All personnel are then required to complete the maintenance history record.

3. Operational Testing of Components

a. Physical Protection Components

Upon completion of the close-out inspection, two equally knowledgeable Physical Security Officers operationally test the components in accordance with written instructions to ensure the proper operation of the component and to verify that the performance capabilities of the component have not been reduced. All personnel are then required to complete the maintenance history record.

b. Interfacing Components

Upon completion of the close-out inspection, a knowledgeable third person from the maintenance group and a Physical Security Officer operationally test the components in accordance with written instructions to ensure proper operation and to verify that the performance capabilities have not been reduced. All personnel are then required to complete the maintenance history record.

4. Training

All security officers receive training in the proper techniques for conducting close-out inspections, detecting collusion by individuals performing maintenance, and for conducting verification and operational checks on components. Additionally, security officers are instructed to immediately bring to the attention of the Security Shift Supervisor any suspicious activities.

IV. AUDITING

The QA/QC Department annually audits the Equipment Checks/ Maintenance Program to ensure compliance with applicable procedures. This audit includes an inspection of each maintenance history record to ensure proper documentation and adherence with approved procedures.

V. VULNERABILITIES

As a minimum, maintenance on physical protection and interfacing components requires a total of five individuals to complete the maintenance, close-out the maintenance activity, and operationally test the component. Collusion between all five individuals is extremely unlikely.

ESCORTS

I. FUNCTION

Escorts provide continuous surveillance of individuals whose access authorization to a MAA requires the presence of an escort.

II. SYSTEM DESCRIPTION

The organization maintains a predetermined inventory of personnel authorized to escort personnel into a MAA. These escorts possess a DOE Q clearance and are assigned an LP-4 Work Designation Code (see Table 18-1). Only personnel possessing an NRC Q or DOE Q clearance are authorized inside a MAA. NRC inspectors possessing a Q clearance (FO-4 Work Designation Code, Table 18-1) do not require an escort.

III. PERFORMANCE CRITERIA

A. Performance Conditions

1. Verifying Clearances

The Security Manager verifies the authenticity of all clearances prior to entering access authorization data into the Personnel Authorization File (PAF) (Reference 1-1).

2. Identification of Personnel Requiring Escorts

All personnel entering the Industrial Security Area (ISA) are required to exhibit a photo ID badge (Reference 62-1). Personnel requiring an escort are issued photo ID badges on a red background.

3. Selection of Escorts

When an escort is required, a Security Officer inputs the control processor to randomly scan the Personnel Authorization File (PAF) and select an LP-4 designated person. Normally, escorts are notified no earlier than 24 hours prior to their assignment.

4. Determining the Number of Escorts

A ratio of one escort to one individual requiring an escort is maintained for MAA admittance. Additionally, when more than two individuals requiring

an escort will be inside the MAA at the same time, a Physical Security Officer will accompany the individuals. A ratio of one Security Officer to two individuals requiring an escort is maintained for admittance into an MAA.

5. Utilizing a Coded Credential Badge

Personnel requiring an escort are issued a coded credential badge (Reference 14-1) in the same manner as the escort. However, during the issuing process, the control processor is programmed to require both coded credential badges to be read by the proximity reader and transferred to the control processor prior to initiating admittance operations. This association process prevents the individual requiring an escort from gaining access to the MAA SAP without the escort being present and the escort from transferring escort responsibilities to another individual. Once inside the MAA SAP, both individuals are required to establish positive personnel identification (see Reference 65-1). Additionally, because the individual requiring an escort utilizes a coded credential badge, the personnel inventory system is continuously updated wtih information relative to the location of the visitor.

6. Escort Training

Prior to being authorized to escort personnel into a MAA, personnel are required to attend an Escort Training Course conducted by the Security Department. This course instructs escorts in proper surveillance techniques and methods of alerting the security force of potential adversary actions.

IV. DETECTION AND ASSESSMENT

A. Detection

1. Escorts are provided with duress alarms (Reference 22-1). These alarms annunciate remotely in the CAS and the SAS.

2. The MAA and the MAA SAP are continously monitored by CCTV (Reference 10-1) from the CAS and the SAS.

3. Facility personnel are instructed, upon contacting an individual with a red background photo ID badge who is not escorted, to immediately inform the CAS

or the SAS and to observe the movements of the individual until a response force arrives.

B. Assessment

A duress alarm is assessed by security officer patrolling the area (Reference 43-1) and by CCTV (Reference 10-1 remotely from the CAS and the SAS.

V. VULNERABILITY

A. Escorts are randomly selected 24 hours prior to being assigned escort responsibilities. Thus, collusion between an insider and one or more outsiders is virtually impossible.

B. Because both individuals must satisfactorily respond to positive personnel identification procedures prior to being admitted to the MAA, the overpowering of an escort prior to MAA SAP admittance serves no purpose. Such activities within the MAA SAP are immediately detected. Resultantly, escorts are not provided with weapons.

EXPLOSIVE DETECTOR HAND-HELD, PACKAGE SEARCH

I. FUNCTION

Packages are searched for the purpose of detecting incendiary and explosive devices being introduced into the MAA.

II. SYSTEM DESCRIPTION

The Ion Track Instruments, Model 70, explosives detector is employed. This unit continuously draws an air sample onto an elastomeric membrane. An argon, carrier gas flows behind the membrane and mixes with the vapors which selectively permeate the membrane. The vapor-argon mixture is then split into two parallel streams. One stream passes through an unobstructed column to an electron capture detector. The other stream passes through a parallel column packed with a substance which selectively retards the flow of the vapor. The amount of retardation depends on the constituents of the vapor. This second column also terminates with an electron capture detector. When the unobstructed column detects the presence of a vapor mixture, the system is programmed to examine the response of the explosive detector's packed column for a fixed period of time. If a detector response from the packed column occurs within this time period, an alarm is sounded. The unit possesses moderate to low specificity and moderate to high sensitivity.

III. PERFORMANCE CRITERIA

A. Site Conditions

All packages are searched inside the MAA SAP (Reference 66-1).

B. Environmental Conditions

1. NO smoking is permitted inside the MAA SAP.

2. Prior to placing the MAA SAP in "open portal" conditions, the MAA SAP is searched for sources of contaminating air or objects which may generate false explosives detector alarms. When possible, such sources are minimized or removed from the area.

C. Performance Conditions

1. Search Procedure

All packages, except those sealed with approved tamper seals (Reference 83-1), are opened and thoroughly inspected using the explosives detector to aid the visual inspection (Reference 88-1). Packages are searched for explosive vapors at each seam and opening. Additionally, the package is compressed slightly with the detector positioned at the most prominent opening to assure sampling of internal vapors. The search procedure requires one to two minutes to complete. Security officers, based on the expected throughput of packages, are not rushed to complete their inspection of packages entering the MAA SAP.

2. Calibration

Explosives detectors are calibrated to detect 200 grams or less of dynamite, TNT, or similar nitrogen compounds with a 90% confidence rate and a false alarm rate not exceeding 1%. Calibration is performed by Technical Security Officers 30 minutes prior to the day shift (DS) (See Table 18-2).

3. Operational Checks

The explosives detector is operationally checked once per hour, utilizing the manufacturer's Nitrogen Test Sample, to ensure proper operation. Security officers performing the operational test exercise care to prevent self-contamination or contamination of the area.

4. Training

Security Officers receive classroom and on-the-job training prior to being authorized to conduct package searches for explosive materials. This training, utilizing written procedures when applicable, includes instructions for properly operating the equipment, proper search techniques, and proper response procedures.

IV. MAINTENANCE AND TESTING

A. Maintenance

All maintenance is performed by Technical Security Officers.

1. Corrective Maintenance

Corrective maintenance is performed on an as-needed basis. Normally, spare explosives detectors are maintained so as to not impede admittance operations while maintenance is being performed.

2. Preventative Maintenance

Preventative maintenance is performed in accordance with the manufacturer's instruction manual.

a. Batteries

The ITI, Model 70, explosives detector utilizes two 13-volt, sealed nickel cadmium batteries and two 6-volt, lead acid batteries. Batteries are inspected on a monthly basis.

b. Membrane

Explosives detector membranes require replacement every two to four weeks.

B. Testing

All tests are performed by Physical Security Officers.

1. Operational tests are conducted hourly (See III.C. 3).

2. Weekly tests, utilizing explosive test samples, are conducted to motivate security officers to perform thorough package searches.

V. DETECTION AND ASSESSMENT

A. Detection

The ITI, Model 70, explosives detector alarms within three to five seconds of the admission of a detectable concentration of nitrogen vapor. The time to clear the detector, after saturation, varies from five seconds to one-and-a-half minutes, depending upon the type of vapors detected.

B. Assessment

When an alarm occurs, the security officer reports the alarm to the CAS and the SAS. The security officer then attempts to locate the object causing the alarm.

If an explosive device, or potential device, is located, the security officer notifies the CAS and the SAS in accordance with Chapter 23 of this plan. If the object causing the alarm cannot be located, the package is removed from the MAA SAP and inspected independently by another security officer and explosives detector. If the alarm is determined to be false, the package is readmitted to the MAA SAP.

The individual desiring access to the MAA is not admitted until the package has been cleared.

VI. VULNERABILITY

The level of detection varies with the type of explosive. In general, electron capture detectors function very well for detecting dynamite, but do not perform well when used to detect other types of explosives. Additionally, countermeasures are available to reduce the amount of vapor available for detection.

EXPLOSIVE DETECTOR HAND-HELD, PERSONNEL SEARCH

I. FUNCTION

Personnel are searched for the purpose of detecting incendiary and explosive devices being introduced into the MAA.

II. SYSTEM DESCRIPTION

The Ion Track Instruments, Model 70, explosives detector is employed. This unit continuously draws an air sample onto an elastomeric membrane. An argon, carrier gas flows behind the membrane and mixes with the vapors which selectively permeate the membrane. The vapor-argon mixture is then split into two parallel streams. One stream passes through an unobstructed column to an electron capture detector. The other stream passes through a parallel column packed with a substance which selectively retards the flow of the vapor. The amount of retardation depends on the constituents of the vapor. This second column also terminates with an electron capture detector. When the unobstructed column detects the presence of a vapor mixture, the system is programmed to examine the response of the explosive detector's packed column for a fixed period of time. If a detector response from the packed column occurs within this time period, an alarm is sounded. The unit possesses moderate to low specificity and moderate to high sensitivity.

III. PERFORMANCE CRITERIA

A. Site Conditions

All personnel are searched inside the MAA SAP (Reference 68-1).

B. Environmental Conditions

1. NO smoking is permitted inside the MAA SAP.

2. Prior to placing the MAA SAP in "open portal" conditions, the MAA SAP is searched for sources of contaminating air or objects which may generate false explosives detector alarms. When possible, such sources are minimized or removed from the area.

C. Performance Conditions

1. Search Procedure

a. All packages and containers carried by the individual are subject to the requirements of Reference 32-1, "Explosive Detector Hand-Held, Package Search."

b. All personnel are thoroughly searched utilizing the explosives detector to aid the visual inspection of the individual. The search includes the areas under the individual's arms, along the inseam and leg portion of the pants, the waist, and the back. Particular attention is given to unusual bulges or bumps under an individual's clothing. Additionally, coats, hats, rubber boots, etc., are removed and inspected separately, after the individual has been inspected. The search procedure requires one to two minutes to complete. Security officers, based on the expected throughput of personnel in an MAA, are not rushed to complete their inspection of personnel entering the MAA.

2. Calibration

Explosives detectors are calibrated to detect 200 grams or less of dynamite, TNT, or similar nitrogen compounds with a 90% confidence rate and a false alarm rate not exceeding 1%. Calibration is performed by Technical Security Officers 30 minutes prior to the day shift (DS) (See Table 18-2).

3. Operational Checks

The explosives detector is operationally checked once per hour, utilizing the manufacturer's Nitrogen Test Sample, to ensure proper operation. Security officers performing the operational test exercise care to prevent self-contamination or contamination of the area.

4. Training

Security Officers receive classroom and on-the-job training prior to being authorized to conduct personnel searches for explosive materials. This training, utilizing written procedures when applicable, includes instructions for properly operating

the equipment, proper search techniques, and proper response procedures.

IV. MAINTENANCE AND TESTING

A. Maintenance

All maintenance is performed by Technical Security Officers.

1. Corrective Maintenance

Corrective maintenance is performed on an as-needed basis. Normally, spare explosives detectors are maintained so as to not impede admittance operations while maintenance is being performed.

2. Preventative Maintenance

Preventative maintenance is performed in accordance with the manufacturer's instruction manual.

a. Batteries

The ITI, Model 70, explosives detector utilizes two 13-volt, sealed nickel cadmium batteries and two 6-volt, lead acid batteries. Batteries are inspected on a morthly basis.

b. Membrane

Explosives detector membranes require replacement every two to four weeks.

B. Testing

All tests are performed by Physical Security Officers.

1. Operational checks are conducted hourly (See III.C. 3).

2. Biweekly tests, utilizing explosive test samples, are conducted to motivate security officers to perform thorough package searches.

V. DETECTION AND ASSESSMENT

A. Detection

The ITI, Model 70, explosives detector alarms within three to five seconds of the admission of a detectable concentration of nitrogen vapor. The time to clear the

detector, after saturation, varies from five seconds to one-and-a-half minutes, depending upon the type of vapors detected.

B. Assessment

When an alarm occurs, the security officer reports the alarm to the CAS and the SAS. The individual is then required to empty his pockets. The security officer then searches the individual again to locate the object causing the alarm. If an explosive device, or potential device, is located, the security officer notifies the CAS and the SAS in accordance with Chapter 23 of this plan. If the object causing the alarm cannot be located, the individual is removed from the MAA SAP and escorted to a search room. An independent search, performed by another security officer and explosives detector is then performed. If necessary, individuals are subject to a pat-down search to locate the object causing the explosives detector alarm.

VI. VULNERABILITY

The level of detection varies with the type of explosive. In general, electron capture detectors function well for detecting dynamite, but do not perform well when used to detect other types of explosives. Additionally, countermeasures are available to reduce the amount of vapor available for detection.

FLOORS, CEILINGS, AND WALLS

I. FUNCTION

Floors, ceilings, and walls provide a capability for detecting, deterring, and delaying a forced entry into a controlled access area. The delay function facilitates assessment and response activities by Security Officers.

II. SYSTEM DESCRIPTION

The MAA and the vault are equipped with emergency exits offering unimpeded egress from the controlled area. Resultantly, physical barriers are employed only for forced entry control.

A. MAA

The floor is below ground level and comprises a portion of the foundation. The walls are inside and the ceiling serves as the floor for the controlled area above the MAA and the vault.

B. Vault

The floor and ceiling of the vault are common with that of the MAA. The walls are inside the MAA.

III. PERFORMANCE CRITERIA

A. Performance Conditions

1. Construction

a. Floor

The floors of the MAA and the vault are constructed of 48-inch thick standard reinforced concrete. The concrete strength is rated at 5,000 psi and is reinforced with eight layers of No. 6 rebar at 6-inch centers.

b. Ceiling

The ceilings of the MAA and the vault are constructed of 24-inch thick standard reinforced concrete. The concrete strength is rated at 5,000 psi and is reinforced with four layers of No. 6 rebar at 6-inch centers.

c. Walls

- MAA

The walls of the MAA are constructed of 36-inch thick standard reinforced concrete. The concrete strength is rated at 5,000 psi and is reinforced with six layers of No. 6 rebar at 6-inch centers.

- Vault

The walls of the vault are constructed of 24-inch thick standard reinforced concrete. The concrete strength is rated at 5,000 psi and is reinforced with four layers of No. 6 rebar at 6-inch centers.

2. Penetration Times

Barrier	Penetration Equipment	Avg. Time (Minutes)
Floor	Explosives (80 pounds) tamper plate, hydraulic bolt cutters	26.5
Ceiling	Explosives (20 pounds) tamper plate, hydraulic bolt cutters	8.8
Walls (MMA)	Explosives (40 pounds) tamper plate, hydraulic bolt cutters	13.6
Walls (Vault)	Explosives (20 pounds) tamper plate, hydraulic bolt cutters	8.8

IV. DETECTION AND ASSESSMENT

The outside perimeter of the MAA is continuously observed by patrolling Security Officers.

A. Open Conditions

When the MAA and the vault are occupied, Security Officers continuously observe the activities of personnel and the status of the physical barriers via CCTV (Reference 10-1).

B. Closed Conditions

The physical barriers of the MAA and the vault are continuously monitored by a microwave (Reference 57-1) detection system. Should the detection system alarm, Security Officers will assess the situation utilizing the CCTV (Reference 10-1) monitoring system.

V. VULNERABILITY

The penetration delay times of the floor, ceiling, and walls are compromised by the presence of entry/exit doors (Reference 21-1), emergency exits (Reference 28-1), and air and utility passages (Reference 3-1).

LOCAL AUDIBLE/VISIBLE ALARMS

I. FUNCTION

Local audible and/or visible alarms provide the capability for indicating the occurrence of an unauthorized activity within a controlled access area or the presence of a hazardous condition to personnel occupying the area.

II. SYSTEM DESCRIPTION

The specific characteristics of each local audible and visible alarm are identified in the detection section of the applicable information response form for a particular component or system. General characteristics, pertinent to all local alarm systems, are contained in this information response form.

III. PERFORMANCE CRITERIA

A. Site Conditions

Local alarms are located such that they satisfy their stated function in the most effective manner. Siting characteristics take into consideration physical barriers, the nearness of bright lights which could dampen the effect of a visible alarm, and elevated background noises which could dampen the effect of audible alarms.

B. Environmental Conditions

1. Natural

The Vital Area (VA), MAA SAP, MAA, and vault are each located inside the facility. Resultantly, natural phenomenon is not expected to adversely affect the proper operation of local audible and/or visible alarms.

2. Man-made

Prior to the selection of a local alarm, the effect of all man-made environmental conditions on the proper operation of the local alarm is identified and evaluated. Consequently, adverse environmental conditions affecting the proper operation of a local alarm are negated during the selection process.

C. Performance Conditions

1. Design Requirements

a. Audible Alarms

Audible alarms have an intensity of at least 15 dB above ambient noise levels at a distance of 10 feet.

b. Visible Alarms

Security visible alarms are bright, flashing strobe lights. Visible alarms indicating personnel hazards are comprised of normal-intensity flashing and nonflashing lights. The color of the light varies depending upon the type of hazard to personnel.

2. Alarm Monitoring

All security alarms are monitored in the CAS and the SAS. The criticality and fire alarms are also monitored remotely in the CAS and the SAS.

3. Power Supplies

Local audible and/or visible alarms are provided with both UPS (Reference 85-1) and Emergency Generating Systems (Reference 29-1) as backup power supplies. Upon a loss of normal power, local alarms switch to the UPS within 1/60 of a second. Once the EGS is prepared to assume the full load, approximately 15 seconds, local alarms automatically switch to the EGS, also within 1/60 of a second. UPS can carry all critical loads for a period of one hour. The EGS can carry all critical loads for a period of 30 days.

4. Resetting Alarms

Security local alarms are only reset by Physical Security Officers with the concurrence of the CAS and SAS. Local alarms associated with hazards to the health and safety of personnel are only reset by individuals responsible for the equipment, such as Health Physics personnel. In all cases, the Facility Shift Supervisor and the CAS/SAS are appraised of the situation surrounding the annunciation of the alarm.

IV. MAINTENANCE AND TESTING

A. Maintenance

Maintenance on security local alarms, both corrective and preventative, is performed by Technical Security Officers. See each specific information response form for the maintenance requirements for a particular component or system. In all cases, maintenance on security-related local alarms is performed in accordance with the manufacturer's instructions and a Mean-Time-Between-Failure (MTBF) schedule.

B. Testing

Testing of security local alarms is performed by Physical Security Officers. See each specific information response form for the testing requirements for a particular component or system. In all cases, components or systems are tested, as a minimum, at least once a week and normally daily.

V. RESPONSE

A. Facility Personnel

All personnel issued a yellow (Company employee) or light blue (Visitor, escort not required) Photo ID Badge (Reference 62-1) receive instructions concerning the proper response to both security and health and safety-related local audible and/or visible alarms. Instructions are conveniently posted throughout the facility.

B. Security Personnel

1. Remote

Security personnel in the CAS/SAS assess the alarm condition via CCTV (Reference 10-1).

2. Local

Local response and assessment is performed by security officers patrolling the area of the alarm (Reference 43-1) and the security response force.

VI. VULNERABILITIES

All security local audible and/or visible alarms are provided with tamper indicating circuitry (Reference 82-1).

MOTION DETECTORS - INTERIOR MICROWAVE SYSTEMS

I. FUNCTION

The microwave detection system provides the capability for detecting adversary activities within a controlled access area during closed portal conditions.

II. SYSTEM DESCRIPTION

The Advanced Device Laboratories (ADL), Model 3300, Microwave Motion Detection System is employed. The motion detection system utilizes a doppler, microwave unit. Movement is detected by a shift in the transmitted frequency. The extent of frequency shift is a function of the size of the target and the speed at which the target is moving through the microwave beam.

III. PERFORMANCE CRITERIA

A. Site Conditions

1. Microwave motion detection units are positioned within the area of coverage such that blind spots on the floor, ceiling, and walls are eliminated. See Reference 38-1 for a physical description of the physical barriers.

2. For controlled access areas having a height of 20 feet or less, microwave units are normally positioned at a height varying from 12 to 14 feet. A minimum of nine feet is always maintained, unless lower levels are specifically required. For controlled access areas having a height of 21 feet or greater, microwave units are positioned to provide multiple detection levels.

B. Environmental Conditions

1. Man-made

a. Man-made environmental conditions, including temperatures, are all controlled such that they do not adversely affect the proper operation of the microwave detection units. The ADL microwave detection unit functions between -20 and +120 degress Fahrenheit with almost zero false alarm rate.

b. EMI protection is provided by restricting RF radiating equipment inside the controlled access area during closed portal conditions. Fluorescent lighting fixtures are not positioned within five feet of a microwave motion detection unit.

2. Natural

The Vital Area (VA), MAA SAP, MAA, and vault are each located inside the facility. Resultantly, natural phenomenon are not expected to adversely affect the proper operation of the ADL Microwave Detection System. Lightning protection is provided by the facility design considerations and power line filtering.

C. Performance Conditions

1. Power Supplies

Each microwave detection unit contains a 12-volt rechargeable battery that is capable of operating the unit for four hours upon a loss of normal power. Additionally, microwave detection units are connected to the Emergency Generating System which is capable of providing electrical power within 15 seconds of a loss of normal power and for a period of 30 days.

2. Installation

All microwave detection units are mounted on stable surfaces, such as the wall or ceiling (Reference 38-1).

3. Operations

Microwave detection units are only operated during closed portal conditions. Units are positioned and adjusted such that the area of coverage is overlapped.

4. Interference

Microwave beams are adjusted such that one beam does not interact with another microwave detection unit.

5. Reliability

The ADL Microwave Detection System has a greater than 99% probability of detection and less than 0.5% probability of initiating a false alarm.

6. Diversity and Redundancy

The CCTV Video Motion Detection System (Reference 11-1), during both opened and closed portal conditions, provides redundant and diverse motion detection in controlled access areas. Additionally, security force officers continuously patrol the peripheral areas of the controlled access area (Reference 43-1).

IV. DETECTION AND ASSESSMENT

A. Detection

The ADL Microwave Detection System is capable of detecting a three-square foot object moving within the controlled access area at a rate varying from 3 inches per second to 10 miles per hour. When motion is detected, the microwave unit annunciates audibly and visually, both remotely and locally. Remote annunciation is in the CAS/SAS.

B. Assessment

1. Remote Assessment

Each microwave unit is connected to a CCTV camera (Reference 11-1), when motion is detected, the CCTV camera is automatically activated to produce a visual display of the area in which motion was detected. Remote alarm assessment of an alarm condition or potential adversary action is performed by the CAS/SAS.

2. Local Assessment

Local assessment is performed by security officers patrolling the VA and by response personnel (Reference 43-1).

V. MAINTENANCE AND TESTING

A. Maintenance

All maintenance is performed by Technical Security Officers.

1. Corrective Maintenance

   Corrective maintenance is performed on an as-needed basis. Spare parts and components are maintained in supply to minimize the downtime of a microwave detection unit.

2. Preventative Maintenance

   Preventative maintenance is performed in accordance with a Mean-Time-Between-Failure (MTBF) schedule and the manufacturer's instruction manual. Normally, maintenance is performed every six months.

B. Testing

1. The Microwave Detection System is tested each time the controlled access area is placed in a closed portal condition. In the event the closed portal conditions is for a period exceeding one week, the Microwave Detection System is tested on a weekly basis. Tests are conducted by a walk-through procedure.

2. Each Microwave Detection System is self-supervised. In the event of a system failure or a loss of power, the microwave detection unit initiates an alarm in the CAS/SAS.

VI. VULNERABILITIES

A. All critical components are located within the controlled access area.

B. Tamper protection is accomplished in the following manners:

1. Each microwave detection unit is monitored by the Video Motion Detection System.

2. Microwave detection units are self-supervised.

3. Access to a microwave detection unit is through the beam of another microwave detection unit.

PHOTO IDENTIFICATION BADGE

I. FUNCTION

The photo I.D. badge is utilized for personnel identification in areas where positive personnel identification is not required. These areas include the Industrial Security Area (ISA), the Protected Area (PA), and the Vital Area (VA).

II. PHOTO I.D. BADGE DESCRIPTION

Each photo I.D. badge is made of Polaroid film. Badges are of standard credit card size and slotted to accommodate clasps and necklaces. Photographs are of sufficient size and quality to allow ease in identifying personnel. The employee's name and employee number is readily visible on the lower half of the Polaroid film. Each badge is laminated.

Background Colors

Personnel Classification	Color
a. Company employee, escort not required	Yellow
b. Visitor, escort not required	Light Blue
c. Visitor, escort required	Red

III. PERFORMANCE CRITERIA

All personnel are issued photo I.D. badges.

A. Performance Conditions

1. Initial Issue

To be issued a photo I.D. badge, a Photo I.D. Badge Request Sheet must be completed. The request sheet requires the signature of the following personnel or their designee:

a. Personnel Administrator - Assigns the individual an employee number or declares the individual a "Visitor."

b. Industrial Safety Supervisor - In-house safety precaution indoctrination.

c. Health Physics Supervisor - Radiation safety precaution indoctrination. The individual is

also scheduled or exempted from the next in-house radiation safety training class.

d. Emergency Coordinator - Emergency preparedness indoctrination.

e. Security Supervisor - Security indoctrination. If the individual is declared a "Visitor," the Security Supervisor determines if the person requires an escort.

Upon completion of the request sheet, the individual is issued a photo I.D. badge. The Security Officer issuing the photo I.D. Badge is responsible for entering the request sheet in the photo I.D. badge inventory file.

2. Daily Issue

Personnel receive their photo I.D. badge when they report to work each day. Upon entering the main gate, the individual requests his badge by giving the Security Officer his employee number. The Security Officer, after obtaining the photo I.D. badge, makes a facial comparison between the facial characteristics displayed on the photo I.D. badge and that of the individual. The Security Officer, situated within an arms reach of the individual while conducting the identity verification, may take as much time as required to make a facial comparison.

Personnel wearing articles not displayed on the photo I.D. badge, such as hats or sunglasses, must remove these articles prior to the Security Officer confirming facial characteristics.

3. Identity Verification at Entry Control Points

a. Security Officers performing identity verification are not assigned concurrent responsibilities.

b. Obtaining admittance to a controlled access area requires the use of the coded credential badge (Reference 14-1). This action initiates a scan of the PAF and the AAF by the control processor. Access authorization results in the name and employee number of the individual to whom the coded credential badge was issued being displayed on the communications terminal at the entry control point. The Security

Officer compares this information with the name and employee number displayed on the photo I.D. badge. Next, a comparison is made of facial characteristics. The facial comparison is made as identified in 2 above.

4. Badge Retention

All personnel exiting the main gate are required to return their photo I.D. badge to the main gate Security Officer. Photo I.D. badges are stored in holders according to numerical employee numbers.

5. Accountability

The Security Department is responsible for all photo I.D. badge system equipment, issuing photo I.D. badges, and maintaining a record of all badges issued.

IV. EFFECTIVENESS OF ENTRY CONTROL PERSONNEL

A. Frequent tests are conducted to motivate Security Officers to detect deviations between an individual's facial characteristics and those displayed on the photo I.D. badge.

B. Security Officers assigned entry control functions not requiring positive personnel identification are not normally rotated. This practice increases the Security Officer's ability to associate the names and facial features of personnel entering the controlled access area.

C. Security Officers receive training in recognizing distinct facial features. This training is conducted on-site and in accordance with NUREG-0464, "Site Security Personnel Training Manual."

V. SYSTEM VULNERABILITY

Photo I.D. badges are fairly easy to duplicate or counterfeit. Resultantly, photo I.D. badges are not utilized as an instrument for gaining access to a controlled area. They are only used as a mechanism for identifying personnel when positive personnel identification is not a requirement.

Vulnerability to duplication or counterfeiting is reduced by retaining photo I.D. badges on the plant site.

POSITIVE PERSONNEL IDENTIFICATION

I. FUNCTION

The system verifies the identification of personnel being issued coded credential badges and reverifies the identification of personnel desiring admittance to designated controlled access areas.

II. SYSTEM DESCRIPTION

A Texas Instruments, Model TI-990, Voice Verification System (VVS) is utilized to establish positive personnel identification. The system is composed of a centrally located "host" computer and several peripheral mini-computers. The "host" computer maintains a 16 word voice print on all AGNS employees and selected visitors. It has a capacity of 1,000 people. The peripheral mini-computers, when activated, make the actual voice print comparisons. The rejection rate for valid personnel identification is 1.0% error. The acceptance rate for invalid personnel identification is 2.0% error. The processing time averages 15 to 20 seconds per person.

III. PERFORMANCE CRITERIA

A. Site Conditions

The "host" computer is located within the CAS. A redundant "host" computer is located within the SAS. Mini-computers are located at the main gate to the Industrial Security Area (ISA) and at each MAA Secured Access Portal (SAP).

B. Environmental Conditions

Components of the VVS are located within atmospherically controlled enclosures. Environmental conditions are not expected to adversely affect the operation of the VVS.

C. Performance Conditions

1. Operation

a. Main Gate ID Verification

When an individual enrolls a coded credential badge into the Schlage Access Control System (Reference 14-1), he enters his employee number on the control processors communications

terminal. This action inputs the VVS which requests the individual to repeat, from the inventory of 16 prerecorded words, a randomly selected sequence of four words. A satisfactory response inputs the VVS to signal the control processor that positive personnel identification has been established. The individual is given 4 opportunities to match the voice print before a rejection alarm is initiated.

b. MAA SAP ID Reverification

When an individual utilizes the coded credential badge to gain admittance into a MAA SAP, the control processor inputs the VVS with the employee number of the individual to whom the coded credential badge was issued at the main gate. The VVS then requests the individual to repeat a randomly selected sequence of four words. A satisfactory response inputs the VVS to signal the control processor that positive personnel identification has been established. The individual is given four opportunities to match the voice print before a rejection alarm is initiated.

2. System Interfaces

The VVS interfaces with the Access Control System (Reference 14-1) to establish positive personnel identification when such identification is a criteria for access authorization.

3. Protective Features

a. Voice Print Matching Program

Access to the voice verification matching program requires access codes. These codes are retained by Texas Instruments.

b. Enrollment of Voice Prints

Voice prints are enrolled into the VVS within the CAS. Only master computer operators possess the codes required to input the "host" computer with individual voice prints.

4. Redundant Equipment

a. Mini-computers

In the event a mini-computer fails, replacement computers are available. Additionally,

individuals may be escorted by physical security officers to the main gate where a positive personnel identification is established. The individual is then escorted back to the MAA SAP by a physical security officer.

b. "Host" Computer

When the "host" computer fails, a backup "host" computer is placed "on-line."

IV. MAINTENANCE AND TESTING

A. Maintenance

All maintenance is performed by technical security officers

1. Corrective Maintenance

Corrective maintenance is performed as necessary.

2. Preventative Maintenance

Preventative maintenance is performed once every six months.

B. Testing

All testing is performed by physical security officers. Each mini-computer is tested once per week by presenting invalid personnel identification and verifying the proper operation of the VVS and associated rejection alarms.

V. DETECTION AND ASSESSMENT

A. Detection

Four unsatisfactory responses or a failure to respond to the VVS within 15 seconds actuates a local and remote alarm with both audible and visual indications. The remote alarm occurs in the CAS and the SAS.

B. Assessment

1. Local

Local alarm assessment is conducted by security officers patrolling the area of the alarm. See Reference 43-1.

2. Remote

Remote assessment, via CCTV (Reference 10-1), is conducted from the CAS and the SAS by security officers.

VI. RESPONSE

A. Active Adversary Action

When assessment of the rejection alarm detects an adversary action, the response is in accordance with the contingency plan (Reference 16-1).

B. No Adversary Action

The individual is requested to exit the MAA SAP and report to the main gate where positive identification attempts are instituted under the guidance of security personnel.

VII. VULNERABILITIES

The VVS is one of the most difficult positive personnel identification systems to compromise.

SECURED ACCESS PORTAL

I. FUNCTION

The Secured Access Portal (SAP) provides the capability of isolating personnel traveling between two controlled access areas for the purpose of conducting ingress or egress functions, such as verifying personal authorization and identification, verifying material authorizations, and conducting contraband searches.

II. SYSTEM DESCRIPTION

Each SAP is custom made based upon the restraints of the placement location within the facility. The MAA SAP measures 10 feet wide, 15 feet long, and 10 feet high. The following equipment, pursuant to both egress and admittance functions, is located within the MAA SAP:

A. A communications terminal.

B. Contraband detection equipment: a hand-held explosives detector (References 32-1 and 33-1), a hand-held weapons detector (Reference 92-1), a walk-through shielding detector (Reference 72-1), and a hand-held SNM detector (References 74-1 and 75-1).

C. A Voice Verification System (VVS) (Reference 65-1).

D. An Access Control System proximity reader (Reference 14-1).

E. CCTV (Reference 11-1).

F. A Microwave Motion Detection unit (Reference 57-1).

III. PERFORMANCE CRITERIA

A. Site Conditions

The MAA SAP is located in accordance with Figure 18-1.

B. Environmental Conditions

1. No smoking is permitted inside the MAA SAP.

2. Only incandescent lighting is utilized.

3. The environmental conditions are controlled such that the proper operation of equipment located inside the portal is not adversely affected.

C. Performance Conditions

1. Physical Protection Capabilities

The MAA SAP is totally within the confines of the Vital Area (VA) and does not comprise any facet of the MAA physical barrier. Additionally, the only purpose of the MAA SAP is to isolate personnel during admittance functions. Resultantly, the MAA SAP does not satisfy any physical protection requirements for the MAA. The only physical protection requirement is that the portal offers sufficient resistance to intrusion so as to allow the security officer inside the MAA SAP to shut MAA-1.1, should an intrusion occur at the same time the door is open.

2. Portal Construction

The MAA SAP is constructed of two 20-guage sheet-metal layers supported by 2 1/2-inch steel framing and provided with 6 inches of fiberglass insulation between the layers. The portal does not contain any windows. Doors are standard industrial, 1 1/2 inch hollow metal core fire doors rated at 1-1/2 hours. Door hinges are located inside the MAA SAP.

3. Door Locking Mechanism

Two active dead bolt systems per door are employed. The active dead bolts, each a 1/2-inch steel rod, and the actuators are positioned inside the frame. One dead bolt is controlled by the Access Control System (Reference 14-1) and the other by the security officer inside the MAA SAP.

4. Penetration Times

Barrier	Penetration Equipment	Average Time (Seconds)
Portal, Door, and Deal Bolt	Hand Tools	10

IV. DETECTION AND ASSESSMENT

A. Detection

1. Closed Portal Conditions

During closed portal conditions, an adversary is detected upon entering the MAA SAP by a microwave detection system (Reference 57-1). The sensor

annunciates audibly in the MAA SAP and audibly and visually in the CAS and the SAS.

2. Open Portal Conditions

a. Inside the MAA SAP

During open portal conditions, an adversary action inside the MAA SAP is detected by one or more of the following:

(1) Direct reporting of the security officer via the communications terminal

(2) Involuntary reporting by the security officer's duress alarm (Reference 22-1)

(3) CCTV monitoring (Reference 11-1) from a remote location, either the CAS or the SAS

(4) Recognition of an invalid voice print by the Voice Verification System (Reference 65-1)

(5) Recognition of an unauthorized person attempting to gain MAA admittance by the Access Control System (Reference 14-1).

Information concerning the annunciation of alarms for each component or system is contained in the specified reference.

b. Outside the MAA SAP

During open portal conditions, an adversary action outside the MAA SAP is detected by one or more of the following:

(1) Guard Force Patrols (Reference 43-1).

(2) CCTV monitoring (Reference 11-1). Both the security officer inside the MAA SAP and the CAS and the SAS possess the capability of monitoring the exterior areas of the MAA SAP.

(3) Recognition of an unauthorized person attempting to gain MAA SAP admittance by the Access Control System (Reference 14-1).

Information concerning the annunciation of alarms for each component or system is contained in the specified reference.

B. Assessment

1. Remote Assessment

An alarm condition or potential adversary action inside or outside the MAA SAP is assessed by CCTV (Reference 11-1) from the CAS and the SAS.

2. Local Assessment

Local assessment is performed by security officers patrolling the Vital Area (VA), including the exterior areas of the MAA SAP. Additionally, the security officer has the capability to assess potential adversary action outside the MAA SAP via CCTV (Reference 11-1).

V. VULNERABILITIES

The MAA SAP is extremely vulnerable to intrusion. Penetration times take only a few seconds. However, CCTV allows the security officer to observe the outside of the MAA SAP continuously. Prior to requesting the CAS or the SAS de-energize the first MAA-1.1 door lock, the security officer ensures no adversary action is occurring exterior to the MAA SAP. Additionally, the CAS and the SAS can view the entire exterior of the MAA SAP prior to de-energizing the first door strike an allowing MAA-1.1 to be opened. Resultantly, penetration times are sufficiently increased to satisfy the stated physical protection performance capabilities of the MAA SAP.

SHIELDING DETECTOR - WALK THROUGH

I. FUNCTION

Personnel are searched for the purpose of detecting weapons, hand tools, and other types of metals which could be utilized for shielding SNM.

II. SYSTEM DESCRIPTION

The Solco, Model IX, shielding detector is employed because of its capacity to function as both a shielding and weapons detector. The unit operates at 24 kHz, producing a magnetic field oriented in the direction of personnel travel through the detector. This field is produced by a transmitter coil positioned at the center of the structure and checks for carried metallic objects. A receiver coil is mounted on each side of the transmitter coil and parallel to it. The unit has a self-balancing network that compensates for metallic objects placed in the vicinity of the detector. Additionally, a movable mechanism mounted within the detector side panel can be used to adjust for imbalances too large to be compensated for with the self-balancing network. Sensitivity of the detector is adjustable via a front panel control. Phase detection techniques permit optimization of detection for either ferrous or nonferrous metals.

III. PERFORMANCE CRITERIA

A. Site Conditions

1. The Solco detector is located inside the MAA SAP (Reference 68-1).

2. The Solco detector is not positioned in a manner which prevents bypassing the detector and it does not confine personnel being screened. However, the MAA SAP is continuously manned by a security officer to ensure personnel pass through and that objects are not passed around the detector.

B. Environmental Conditions

1. X-ray detectors are not utilized at the MAA SAP for the inspection of packages or containers. All packages and containers entering the Protected Area (PA) are inspected by X-ray detectors.

2. The only metal object of significance, inside the MAA SAP (Reference 68-1), is the MAA entrance door (MAA-1.1). The Solco detector is positioned in excess of three meters from the entrance door. All metal objects and structural material are rigidly positioned. During contraband searches, the doors are locked.

3. Air conditioning compressors and similar types of electrical equipment which periodically switch "on" and "off" are not located within the MAA SAP or in the immediate area.

4. Only incandescent light fixtures are utilized inside the MAA SAP.

5. The MAA SAP environment, including temperature, is controlled such that the environment does not adversely affect the proper operation of the Solco detector.

6. The other devices utilized to detect contraband inside the MAA SAP do not generate electronic fields which interfere with the detection capabilities of the Solco detector.

C. Performance Conditions

1. Search Procedure

Except when an individual requires an escort, only one person is allowed inside the MAA SAP at a time. To ensure this capability, the security officer has the capability of locking MAA-1.1 and the entrance to the MAA SAP during admittance functions.

a. All packages and containers carried by the individual are subject to the requirements of Reference 92-1, "Weapons Detector - Hand Held, Package Search."

b. The security officer inside the MAA SAP ensures that all pesonnel desiring access to the MAA adhere to written admittance procedures. Personnel are required to remove their shoes (only if steel-toed) and empty their pockets prior to passing through the detector. Fiberglass lockers are provided for the storage of personal articles while the individual is inside the MAA. Additionally, the company provides personnel entering the MAA with work clothes which are free of metal objects. As the individual passes through the Solco detector, he is required to stand motionless in the

middle of the detector for three seconds. During the admittance procedure, the security officer is not distracted from observing the actions of the individual and has the capability of face-to-face communications. The expected throughput of personnel, normally one individual at a time, does not require multiple detection units inside the MAA SAP.

2. Calibration

The Solco detector is calibrated to detect 100 grams or less of nonferrous metal located anywhere on the individual with a 90% confidence rate and a false alarm rate not exceeding 1%. Calibration is performed by Technical Security Officers 30 minutes prior to the day shift (DS) (See Table 18-2).

3. Performance Testing

Performance testing is conducted during the calibration.

a. As a Weapons Detector

A "clean" tester carries a 200 gram, nonferrous test sample, either brass, copper, or aluminum, through the center of the detector at one meter/second. Four passes, each initiating an alarm, are required. Similarly, the "clean" tester carries a forbidden detection item through the detector four times without causing an alarm. Passing these two tests indicates adequate performance.

b. As a Shielding Detector

A "clean" tester carries a 100 gram, right circular, lead cylinder through the center of the detector at one meter/second. Four test passes, each initiating an alarm, indicate adequate performance.

4. Operation Checks

The Solco detector is operationally checked once per hour, utilizing a 100 gram, right circular, lead cylinder. The cylinder is passed through any portion of the detector to ensure its sensitivity. This minimum shielding test exceeds and satisfies the minimum weapons test for sensitivity.

5. Training

Security officers receive classroom and on-the-job training prior to being authorized to conduct personnel searches for weapons and shielding materials. This training, using written procedures when applicable, includes instructions for properly operating the equipment, proper search techniques, proper response procedures, and proper methods of observing personnel attempting to exploit detector vulnerabilities.

6. Prohibited Articles

Personnel are instructed to not carry items which routinely cause the Solco detector to alarm. Lists of such items, such as keys, coins, pocket knives, belt buckles, watches, etc., are posted at the entrance to all MAA SAP's.

7. Interference

a. RF Transmissions

With the exception of the duress alarms (Reference 22-1), all communications utilize the communications terminal located inside the MAA SAP. The duress alarm only transmits during a stress condition.

b. Line Voltage Variations and Transients

Tests indicate that the Solco, Model IX, detector is not sensitive to line voltage variations between 110 and 130 volts. To prevent false alarms resulting from voltage transients, the Solco detector is connected to an independent, protected line.

IV. MAINTENANCE AND TESTING

A. Maintenance

1. Corrective Maintenance

Corrective maintenance is performed on an as-needed basis. A spare Solco, Model IX, detector is available when the installed detector requires maintenance. When electrical power is lost to the detector and admittance is required, hand-held weapons detectors (Reference 92-1), utilized for package searches, are used for personnel searches.

2. Preventative Maintenance

Preventative maintenance is performed in accordance with the manufacturer's instruction manual.

B. Testing

All tests are performed by Physical Security Officers (see III.C.3 and III.C.4 above).

V. DETECTION AND ASSESSMENT

A. Detection

The Solco, Model IX, detector alarms almost instantaneously upon the admission of a detectable quantity of metal passing through the magnetic field.

B. Assessment

When an alarm occurs, the security officer reports the alarm to the CAS and the SAS. The individual is then reinstructed to empty his pockets or remove any metal objects from his person and, after the alarm condition has reset, to pass through the detector again. If the detector continues to alarm, the individual is removed from the MAA SAP and escorted to a search room. The individual is then searched again using another Solco, Model IX, detector. If necessary, the individual is subjected to a pat-down search to locate the object causing the alarm.

If a weapon or shielding container is detected, the security officer notifies the CAS and the SAS in accordance with Chapter 23 of this plan.

VI. VULNERABILITY

All weapons and shielding detectors can be defeated by rapidly passing an object through the detection field. However, security officers manning the MAA SAP ensure personnel remain in the magnetic field for three seconds. Additionally, the detector is not desensitized at the floor to allow the passage of steel-toed safety shoes.

TAMPER-INDICATING CIRCUITRY

I. FUNCTION

Tamper-indicating circuitry provides the capability for detecting malfunctioning components or transmission lines and attempts to compromise the validity of security data.

II. SYSTEM DESCRIPTION

Tamper indications are provided by two kinds of tamper-indicating systems: tamper-indicating switches and supervisory current systems. Tamper-indicating switches prevent an adversary from gaining access to the internals of a component without initiating an alarm. Supervisory current systems detect an adversary action which adds or deletes impedance (AC system) or resistance (DC systems) from a system, such as bypassing a component which could initiate an alarm.

III. PERFORMANCE CRITERIA

A. Site Conditions

Tamper-indicating circuitry systems utilize signal lines which are located within the Protected Area (PA), as a minimum. Normally, the majority of tamper-indicating circuits are located in the same controlled access area as the component protected by the circuitry, such as the MAA or the vault.

B. Environmental Conditions

Environmental conditions are controlled such that they do not adversely affect the proper operation of the tamper-indicating circuitry.

C. Performance Conditions

1. Installation

All signal lines are enclosed in conduit and buried in concrete.

2. Operation

Both the supervisory current systems and the tamper-indicating switches provide continuous tamper-indicating capabilities

3. Alarms

Tamper-indicating alarms are maintained separate from the alarms generated by the component being protected. Alarms are initiated in both the secure and access modes.

4. Power Supplies

The power supply to the tamper-indicating circuitry is the same power as supplied to the component being protected. See Reference 85-1 for components connected to the UPS system and Reference 29-1 for components connected to the EGS system. Upon a loss of power, components protected by supervisory current systems indicate a tamper alarm.

IV. DETECTION AND ASSESSMENT

A. Detection

1. Tamper-Indicating Switches

Tamper-indicating switches alarm when an attempt is made to open the component's enclosure. The alarm annunciates both audibly and visually in the CAS/SAS.

2. Supervisory Current

Supervisory current systems can be adjusted to alarm whenever the system's current changes by a specified percentage. Percentages range from 5% to 20%. The alarm annunciates both audibly and visually in the CAS/SAS.

B. Assessment

1. Remote Assessment

An alarm condition or potential adversary action is assessed remotely by CCTV (Reference 11-1) from the CAS/SAS.

2. Local Assessment

Local assessment is performed by security officers patrolling the VA (Reference 43-1) and response personnel.

V. MAINTENANCE AND TESTING

A. Maintenance

1. Corrective Maintenance

Corrective maintenance is performed on an as-needed basis. Spare parts and components are maintained in supply to minimize downtimes.

2. Preventative Maintenance

Preventative maintenance is performed semiannually or when warranted by Mean-Time-Between-Failure (MTBF) schedules, at more frequent intervals.

B. Testing

Tamper-indicating circuits are tested whenever maintenance is performed on the component. As a minimum, tests are conducted at least once per month.

VI. VULNERABILITY

A. Tamper-indicating switches are spring loaded to the alarm position. The component cannot be opened without generating the tamper alarm.

B. Supervisory current systems detect either the addition or deletion of impedance to the component. Consequently, detection devices cannot be bypassed or removed from the system without initiating the alarm. Adjusting the current change form 5% to 20% affects the sensitivity of the system to current changes in the component.

VII. EQUIPMENT PROTECTED

A. CCTV (Reference 11-1)

B. Controlled security lighting (Reference 17-1)

C. Local audible and visual alarms (Reference 51-1)

D. Microwave Motion Detection System (Reference 57-1)

TAMPER SEALS AND INSPECTIONS

I. FUNCTION

Tamper seals and inspections prevent utilizing the internal areas of instruments and similar components to introduce contraband into or to remove SNM from a MAA and/or vault.

II. SYSTEM DESCRIPTION

The tamper seals utilized are similar to seals used to ensure the integrity of SNM containers. Tamper seals are constructed of sheet vinyl or paper with a pressure-sensitive backing. Seals are procured with consecutive serial numbers which take the form of either printed or perforated dots.

III. PERFORMANCE CRITERIA

A. Site Conditions

Tamper seals are positioned upon the instrument or component so that at least one inch overlaps either side of the container's parting line. A sufficient number of seals are strategically positioned to prevent opening the component without violating the integrity of at least one of the tamper seals.

B. Environmental Conditions

Environmental conditions do not adversely affect the performance of the tamper seal.

C. Performance Conditions

1. Issuing and Installation

a. Issuing

Personnel desiring to introduce instrumentation or similar components into the MAA or the vault are required to submit a Security Work Order (SWO) (Reference 98-1) to the security supervisor. The SWO identifies components which are impractical to disassemble for inspection within the MAA SNP. Upon approving the SWO, the security supervisor informs the tamper seal custodian of any instrumentation requiring a tamper seal and the shift for which the entry is scheduled. The tamper seal custodian initiates the installation process on the day

shift (DS) preceding the shift in which the instrument has been authorized MAA or vault admittance.

b. Installation

Prior to installing the seal, the component is disassembled, inspected, and reassembled by a technical security officer in the presence of the tamper seal custodian. Upon satisfactory completion of the inspection, the tamper seal custodian, in compliance with the Site Conditions (III.A), positions the required number of tamper seals upon the component.

2. Tamper Seal Inventory

a. Recording Issued and Installed Seals

Upon installing a tamper seal(s), the tamper seal custodian records the seal's serial number and the component's name and serial (identification) number in the Tamper Seal Inventory Log. This information is then entered into the computer communications central storage file along with the SWO (Reference 98-1).

b. Recording Destroyed Seals

Upon receipt of a destroyed seal, the tamper seal custodian records the date returned in the Tamper Seal Inventory Log and retains the seal in a Destroyed Seals File.

c. Accountability Inventory

On a monthly basis, a physical security officer in the presence of the tamper seal custodian, conducts an inventory of all destroyed and unused tamper seals. This inventory includes all tamper seals presently installed on components inside a MAA or vault.

3. MAA SAP Inspection

a. Entering Inspection

When a component is presented for introduction into the MAA and/or the vault, the security officer retrieves the SWO from the communications terminal in the MAA SAP. The security officer's inspection includes:

(1) Ensuring the component is being introduced only during the shift authorized on the SWO.

(2) Matching the tamper seal's serial number to that indicated on the communications terminal.

(3) Matching the component's serial number to that indicated on the communications terminal.

(4) Ensuring the integrity of the seal is not violated.

b. Exiting Inspection

When a component exits the MAA, the security officer retrieves the SWO from the communications terminal in the MAA SAP. The security officer's inspection includes:

(1) Matching the tamper seal's serial number to that indicated on the communications terminal.

(2) Matching the component's serial number to that indicated on the communications terminal.

(3) Ensuring the integrity of the tamper seal is not violated.

The security officer then removes the seal(s), attempting to leave the seal's serial number intact, and places it in an envelope. Destroyed seals are returned to the tamper seal custodian.

IV. DETECTION AND ASSESSMENT

A. Detection

The seal material tears extremely easily if attempts are made to remove the seal. Utilizing solvents to remove the seal causes the background ink to run or destroys the seal material.

B. Assessment

Assessment of a violated seal or a seal serial number descrepancy includes:

1. Maintaining the component within the MAA SAP until the cause of the violation is determined.

2. Inspection of the internals of the component.

3. Filing a Security Incident Report.

V. ACCOUNTABILITY

The tamper seal custodian is solely responsible for procuring, storing, inventorying, and issuing tamper seals.

VI. VULNERABILITY

A. Tamper seals of the nature described are the most difficult of all tamper seals to compromise.

B. The tamper seal custodian only has access to the tamper seals. The security supervisor is the only individual authorized to enter SWO information into the communications central storage file. This configuration precludes the authorization and installation of a tamper seal by only one individual.

VAULTS

I. FUNCTION

The vault provides the capability for protecting SNM during periods when the SNM is not being processed, prepared for processing, or transferred to the packaging and loading area. Additionally, the vault provides a capability for aiding in the detection and assessment of an adversary action and in delaying the adversary action to facilitate a response by security personnel.

II. SYSTEM DESCRIPTION

The Plutonium Storage Area (PSA) receives plutonium nitrate (250 grams/liter Pu-3M HNO_3) from the process system and stores the plutonium nitrate in two geometrically favorable storage tanks. Each tank is capable of storing 4,000 kilograms plutonium. See the Final Safety Analysis Report (FSAR) for a complete description of the storage tanks and the materials contained therein. Materials are always stored in the vault unless undergoing processing or being transferred for shipment.

III. PERFORMANCE CRITERIA

A. Site Conditions

1. Refer to Figure 18-1 for a block diagram of the vault.

2. The vault floor rests below grade (Reference 38-1).

B. Environmental Conditions

Environmental conditions within the vault are controlled such that the proper operation of all components within the vault is not adversely affected.

C. Performance Conditions

1. Access Frequency

Frequent admittance to the vault is not expected. Access is only anticipated for radiological surveys and maintenance inspections on a quarterly basis. The transfer of SNM in and out of the vault is via piping systems.

2. Construction of Components

a. Floors, walls, and ceilings (Reference 38-1)
b. Air and utility barriers (Reference 3-1)
c. Door and associated hardware (Reference 21-1)
d. Emergency exits (Reference 28-1)

3. Weakest Element of the Vault

The weakest element of the vault is VAU-1.1 (Reference 21-1). The door is 4 and 1/4 inches thick - 3/4-inch steel plate, 3-inch redwood, and 1/2-inch steel plate. The penetration delay time, utilizing explosives with a tamped charge, is 1.5 minutes.

4. Safeguards Features

a. Authorization Schedules (Reference 1-1)
b. Authorization Procedures (Reference 2-1)
c. CCTV Monitoring/Surveillance (Reference 10-1)
d. CCTV Systems (Reference 11-1)
e. Coded Credential System (Reference 14-1)
f. Controlled Security Lighting (Reference 17-1)
g. Duress Alarms (Reference 22-1)
h. Escorts (Reference 31-1)
i. Local Audible/Visual Alarms (Reference 51-1)
j. Positive Personnel Identification (Reference 65-1)

5. Accessibility of Exterior Surfaces

A three-foot boundary is maintained between the exterior surface of the vault's physical barrier and any components or systems within the MAA to facilitate visual inspection, surveillance, and assessment.

6. Response

The number of personnel responding to an alarm condition and the expected response times are identified in Chapter 23 of the plan.

IV. DETECTION AND ASSESSMENT

A. Detection

1. Closed Portal Condition

a. The Microwave Detection System (Reference 57-1) provides a detection capability during closed

portal conditions. Annunciation is both audible and visual, both remotely and locally. Remote annunciation is in the CAS/SAS.

b. The Video Motion Detection System (Reference 11-1) provides a detection capability during closed portal conditions. Annunciation is both visual and audible in the CAS/SAS.

2. OPEN PORTAL CONDITIONS

a. The Video Motion Detection System (Reference 11-1) provides a detection capability during open portal conditions for all or parts of the vault. Annunciation is both visual and audible in the CAS/SAS.

b. Detection of adversary action is also accomplished by the monitor viewing the CCTV (Reference 11-1) and 10-1) visual display in the CAS/SAS.

B. Assessment

1. Remote Assessment

An alarm condition or potential adversary action is assessed by CCTV (Reference 10-1) from the CAS/SAS.

2. Local Assessment

Local assessment is performed by security officers patrolling the VA (Reference 43-1) and response personnel (See Chapter 23).

V. VULNERABILITIES

The vulnerabilities of each component or system are addressed in each of the specific information request sheets.

PACKAGE SEARCH - VISUAL INSPECTION

I. FUNCTION

Packages are visually searched for the purpose of preventing the introduction of contraband into or the removal of SNM from a controlled access area.

II. SYSTEM DESCRIPTION

Packages entering and exiting a MAA are searched with the aid of an explosives detector (Reference 32-1) and a metal detector (Reference 92-1). Packages exiting the MAA are additionally searched with the aid of an SNM detector (Reference 74-1).

III. PERFORMANCE CRITERIA

A. Site Conditions

All packages destined for the MAA are searched. Normally, this search occurs inside the MAA SAP (Reference 68-1); however, special packages may be searched at a remote location when a Security Work Order (SWO) (Reference 98-1) has been approved.

B. Performance Conditions

1. Package Inspection

a. Packages Searched in Accordance with an SWO

Package searches conducted in a remote location are identical to those searches performed inside the MAA SAP.

b. Packages Searched Inside the MAA SAP

All packages, except those sealed with approved tamper seals (Reference 83-1), are opened and thoroughly searched. The search includes removal of all contents, unwrapping the contents, and inspection of the packing materials. The length of the search depends on the size of the package; however, the size of the package is not a deterrent to thoroughly conducting a search. Security officers, based on the expected throughput of packages, are not rushed to complete their search, nor are they distracted by concurrent responsibilities.

2. Training

Security officers receive classroom and on-the-job training prior to being authorized to conduct visual package searches. This training, utilizing written procedures when applicable, includes instructions for properly operating detection equipment, properly conducting searches, properly responding to contraband, and recognizing explosives, weapons, nuclear materials, and SNM shielding containers and metals.

3. Reliability

a. Remote Location Contraband Searches

To prevent collusion between the individual desiring to introduce a package into the MAA and the individual performing the search, a third security officer is always present at the inspection. See Reference 83-1, Section III.C.1, for a detailed description of the inspection procedures.

b. MAA SAP Searches

To prevent collusion between an individual desiring to introduce a package into the MAA and the individual performing the search, the following precautions are taken:

1. Security officers are randomly assigned entry control responsibilities on a daily basis.

2. Security officers assigned entry control functions work in pairs; one is physically inside the MAA SAP, the other monitors entry control functions remotely by CCTV (Reference 10-1).

4. Admittance Authorization for Materials

During the package inspection, the security officer compares the items submitted for inspection against the items listed on the SWO (Reference 98-1). Any item not identified on the SWO is considered contraband.

IV. TESTING

Weekly tests, utilizing weapons and explosives test samples, shielding containers and metals, and other types

of contraband test samples, are conducted to motivate security officers to conduct thorough package searches.

V. DETECTION AND ASSESSMENT

A. Detection

Detection may be the result of visually identifying contraband or the annunciation of a detector alarm.

B. Assessment

When contraband is suspected or detected, the security officer reports the condition to the CAS and the SAS in accordance with Chapter 23 of this plan. The package is then removed from the MAA SAP and searched at a remote inspection station. If contraband is not detected, the package is returned to the MAA SAP.

The individual desiring access to the MAA is not admitted until the package has been cleared.

VI. VULNERABILITY

Vulnerability is a function of the sensitivity of the detectors utilized, the type of contraband being introduced, and the thoroughness of the inspection.

WEAPONS DETECTOR HAND-HELD, PACKAGE SEARCH

I. FUNCTION

Packages are searched for the purpose of detecting weapons, hand tools, and other types of metals which could be utilized for shielding SNM entering the MAA.

II. SYSTEM DESCRIPTION

Federal Laboratories Inc., Transfrisker Model 6030, weapons detector is employed. The unit operates by producing a magnetic field which detects distortion caused by metal objects. The unit is capable of detecting both nonferrous and ferrous metal objects.

III. PERFORMANCE CRITERIA

A. Site Conditions

All packages are searched inside the MAA SAP (Reference 68-1).

B. Environmental Conditions

1. The MAA SAP is primarily constructed of wood. The only significant metal object inside the MAA SAP is the MAA entrance door (MAA-1.1).

2. The environment of the MAA SAP is controlled such that it does not adversely affect the proper operation of the weapons detector.

C. Performance Conditions

1. Search Procedure

All packages, except those sealed with approved tamper seals (Reference 83-1), are opened and thoroughly inspected using the weapons detector to aid the visual inspection (Reference 88-1). Additionally, all packaging materials are inspected. The search procedure normally requires one to two minutes to complete per package. Security officers, based on the expected throughput of packages, are not rushed to complete their inspection of packages entering the MAA SAP.

2. Calibration

The weapons detector is calibrated to detect 200 grams or less of nonferrous metal located

within 18 inches of the detector probe with a 90% confidence rate and a false alarm rate not exceeding 1%. Calibration is performed by Technical Security Officers 30 minutes prior to the day shift (DS) (See Table 18-2).

3. Performance Testing

Performance testing is conducted during the calibration. A "clean" test package, containing a 200 gram, nonferrous test sample, either copper, brass, or aluminum, is submitted for search. Four test passes, each causing an alarm, are made to indicate proper operation of the detector. Similarly, the test package, containing a forbidden detection item, is passed through the search procedure four times without initiating an alarm. Passing these tests indicates adequate performance.

4. Operational Checks

The weapons detector is operationally checked and balanced once per hour, utilizing a 200 gram, round piece of brass, copper, or aluminum. The test sample is passed within 18 inches of the detector probe.

5. Training

Security officers receive classroom and on-the-job training prior to being authorized to conduct package searches for weapons. This training, using written procedures, includes instructions for properly operating the equipment, proper search techniques, and proper response procedures.

IV. MAINTENANCE AND TESTING

A. Maintenance

All maintenance is performed by Technical Security Officers.

1. Corrective Maintenance

Corrective maintenance is performed on an as-needed basis. Normally, spare weapons detectors are maintained so as to not impede admittance operations while maintenance is being performed.

2. Preventative Maintenance

Preventative maintenance is performed in accordance with the manufacturer's instruction manual. The model 6030 contains two, 9-volt batteries which are inspected during the calibration procedure. A voltage output of 6.5 VDC requires the batteries to be replaced prior to operations.

B. Testing

All tests are performed by Physical Security Officers.

1. Operation and performance tests are conducted in accordance with III.C.3 and III.C.4.

2. Weekly tests, utilizing weapon test samples, are conducted to motivate security officers to perform thorough package searches.

V. DETECTION AND ASSESSMENT

A. Detection

The Transfrisker Model 6030 audibly annunciates almost instantaneously upon the detection of a metal object.

B. Assessment

When an alarm occurs, the security officer reports the alarm to the CAS and the SAS. The security officer then attempts to locate the object initiating the alarm. If a weapon, or potential weapons or shielding object is located, the security officer notifies the CAS and the SAS in accordance with Chapter 23 of the plan. If the object causing the alarm cannot be located, the package is removed from the MAA SAP and inspected independently by another security officer and weapons detector. If the alarm is determined to be false, the package is readmitted to the MAA SAP.

The individual desiring access to the MAA is not admitted until the package has been cleared.

VI. VULNERABILITY

All weapons detectors can be defeated if the detector is passed over a metal object too rapidly. Consequently, security officers are instructed to conscientiously search packages without regard for the length of time necessary for completing the search.

WEAPONS DETECTOR - WALK THROUGH

The Solco, Model IX, shielding detector is employed for the purpose of detecting weapons and metals utilized for shielding SNM. See Reference 72-1 for information concerning the attributes of this detector for detecting weapons entering the MAA.

SECURITY WORK ORDER

I. FUNCTION

The Security Work Order (SWO) relieves entry control personnel of the responsibility for determining what equipment and materials are authorized for admittance into an MAA and vault.

II. SYSTEM DESCRIPTION

The Security Work Order identifies the job to be performed, the time the job is authorized, each component to be introduced, and any components for which tamper seals are requested.

III. PERFORMANCE CRITERIA

A. Performance Conditions

1. Submitting an SWO

Except during emergency conditions, SWO's are required to be submitted to the Security Supervisor at least two days prior to the anticipated date of admittance.

2. Authorizing Materials

When an SWO is submitted, the Security Supervisor checks the Production Schedule to ensure the job is authorized and that the job is authorized at the times indicated on the SWO. The Security Supervisor then verifies the need for the materials based upon his intuition and by checking with a supervisor of the individual desiring to introduce the materials. The Security Supervisor does not authorize any materials until completely satisifed that the materials are required to perform the authorized activity. When conflicts arise which cannot be resolved, the Security Manager and the Plant Manager make the final determination as to the need for the materials.

3. Entering the Inventory Listing

After authorizing the materials, the Security Supervisor assigns the SWO an identification number and enters the inventory listing of authorized materials into the computer communications central storage file. Additionally, the inventory listing

identifies all components which the Security Supervisor has authorized to be sealed with tamper seals.

4. MAA SAP Operations

Individuals desiring to introduce materials into the MAA and vault must carry a copy of the SWO into the MAA SAP. The security officer inside the MAA SAP enters the SWO identification number into the communications terminal. The inventory listing associated with the SWO identification number is then displayed on the communications terminal. The security officer checks the materials presented against the inventory listing. Any materials found which are not listed on the inventory listing are considered to be contraband and report in accordance with procedures for unauthorized materials.

Upon exiting the MAA, the security officer again checks the inventory listing to ensure that only authorized materials are removed from the MAA or vault.

5. Provisions for Utilizing Tamper Seals

Some materials and/or components, such as electrical test instrumentation, are impractical to disassemble and inspect within the MAA SAP. Consequently, the Security Supervisor may authorize tamper seals to be placed on the components. When tamper seals are required, the Security Supervisor sends a copy of the SWO to the Tamper Seal Custodian. In accordance with Reference 83-1, the Tamper Seal Custodian inspects the component and places the required number of tamper seals on the casing.

When the SWO inventory listing identifies components authorized to be sealed with tamper seals, the security officer ensures that the tamper seal identification numbers are valid and that the integrity of the seals has not been violated.

IV. VULNERABILITIES

Only the Security Supervisor is authorized to enter data into the computer communications central storage file. To prevent collusion between the Security Supervisor and the individual desiring access, the following precautions are taken:

A. The control processor prints out a record of all components which have been authorized to be admitted to an MAA and vault. On a daily basis, the Security Shift Supervisors review all component authorizations for their shift. Consequently, the Security Shift Supervisor has the opportunity to question the need for any suspicious components prior to the actual introduction of the component into the MAA and vault.

B. Entry control personnel have the authority to refuse admittance to any components they feel are not required to perform those activities which are authorized inside the MAA and vault.

5.0 EFFECTIVENESS TEST QUESTIONNAIRE ANSWERS

Effectiveness Test Questionnaires (ETQ) assist the NRC in evaluating the Physical Protection Plan's ability to satisfy the performance capability requirements of the Physical Protection Upgrade Rule. This evaluation is performed by answering specific questions, pertinent to the plan's performance capabilities, utilizing graded performance level answers contained in each ETQ. Only the performance level answers are contained in this section. The ETQ forms are contained in the Design Guidance Compendium.

AUTHORIZATION SCHEDULES

ANSWERS

1. A
2. A
3. NO VEHICLES AUTHORIZED
4. NO VEHICLES AUTHORIZED
5. A

AUTHORIZATION PROCEDURES

ANSWERS

1. A
2. A
3. AUTHORIZATION PAPERS NOT UTILIZED, AUTHORIZATION DATA STORED IN PERSONNEL AUTHORIZATION FILE (COMPUTERIZED ACCESS PROGRAM).
4. SEE 3 ABOVE
5. A
6. A (WE WILL UTILIZE MORE DATA)
7. BOTH A & B
8. A
9. A (VISITORS WITHOUT DOE Q OR NRC Q CLEARANCE ARE NOT ADMITTED TO MAA).
10. A (WE WILL UTILIZE MORE DATA)
11. A (SEE CRITIQUE SHEET)
12. NO VEHICLES AUTHORIZED
13. NO VEHICLES AUTHORIZED
14. NO VEHICLES AUTHORIZED
15. B (SEE CRITIQUE SHEET)
16. A
17. A

AIR AND UTILITY INLET BARRIERS

ANSWERS

1. C
2. A
3. B
4.
5. A, B

BALANCED MAGNETIC SWITCHES

ANSWERS

1. A
2. B
3. A
4. A
5. A
6. A
7. A
8. A
9. Opening the door
10. A
11. A
12. D
13. A
14. A
15. A

CCTV

ANSWERS

1. A
2. A
3. A
4. A
5. A
6. A
7. B
8. A
9. A
10. A
11. A
12. A
13. A
14. A
15. A
16. A

CCTV SYSTEMS

ANSWERS

1. A
2. A
3. A
4. B
5. A
6. A
7. B
8. A
9. A
10. A
11. A
12. A
13. A
14. A
15. A
16. A

CODED CREDENTIAL BADGE

ANSWERS

1. A
2. A
3. A
4. A
5. A
6. A
7. A
8. Criteria for answering not available
9. A
10. Criteria for answering not available

CONTROLLED SECURITY LIGHTING

ANSWERS

1. A
2. A
3. D - See Critique Sheet
4. A
5. A
6. A
7. A
8. A
9. A
10. A
11. A

DOORS & ASSOCIATED HARDWARE

ANSWERS

1. A & B
2. A
3. None of the answers are applicable
4.
5.
6. A
7. A
8. A
9. A & B

DURESS ALARMS

ANSWERS

1. C
2. A
3. A
4. B
5. A
6. A
7. C
8. B
9. B
10. Not Employed
11. B
12. A

EMERGENCY EVACUATION PROCEDURES

ANSWERS

1. A
2. A
3. A
4. A
5. A
6. A
7. A
8. A
9. A
10. A
11. A
12. A
13. B
14. A
15. A
16. A
17. C
18. A
19. A

EMERGENCY EXITS

ANSWERS

1. A
2. A
3. A
4. A
5. A
6. A
7.
8. B
9. A
10. A
11. Answer does not correlate to the question
12. A & B
13. B
14. A
15. Criteria for answering not available

EQUIPMENT CHECKS/MAINTENANCE

ANSWERS

1. A
2. A
3. A
4. A
5. A
6. A
7. A
8. A
9. A
10. A

ESCORTS

ANSWERS

1. A
2. A
3. A
4. Answer not provided - See Critique Sheet
5. A
6. A
7. A
8. B

EXPLOSIVES - PACKAGE SEARCH

ANSWERS

1. A
2. A
3. A
4. A
5. A
6. A
7. A
8. A
9. A
10. A
11. A
12. A
13. A
14. A

EXPLOSIVES - PERSONNEL SEARCH

ANSWERS

1. A
2. B
3. A
4. A
5. A
6. A
7. A
8. A
9. A
10. A
11. A
12. A
13. A

FLOORS, CEILING, AND WALLS

ANSWERS

Floors

1. Below grade (answer not provided)
2. A
3. A
4.
5. A
6. A
7. A

Roof

1. A
2. B
3.
4. B
5. A
6. A

Walls

1. A
2. B
3.
4. B
5. A

LOCAL AUDIBLE/VISIBLE ALARMS

ANSWERS

1. A
2. A
3. A, B, C
4. B
5. A
6. A, B
7. B
8. A
9. A
10. A
11. A
12. A
13. A

MOTION DETECTORS

ANSWERS

1. A
2. A
3. A
4. A
5. A
6. A
7. A
8. NOT USED
9. A
10. A
11. A
12. A
13. C
14. D
15. A
16. A
17. A
18. A
19. A
20. A

PHOTO I.D. BADGES

ANSWERS

1. C
2. C
3. A
4. B
5. A
6. A
7. A
8. A
9. A
10. A
11. A
12. A
13. A
14. A
15. A
16. C
17. A (Not performed remotely)
18. A (Not performed remotely)

POSITIVE PERSONNEL IDENTIFICATION

ANSWERS

1. A
2. A
3. A
4. A
5. A
6. A
7. A
8. A
9. N/A See Critique Sheet
10. N/A See Critique Sheet
11. A
12. A
13. A
14. N/A See Critique Sheet

SECURED ACCESS PORTAL

ANSWERS

1. C
2. 10 seconds
3. C
4. A
5. B
6. Not a secured structure because it is outside MAA
7. C
8. C
9. C

NOTE: See plan for description of MAA SAP.

SHIELDING DETECTOR - WALK THROUGH

ANSWERS

1. B
2. A
3. A
4. B
5. B
6. A
7. Answer not provided - See Critique Sheet
8. A
9. A
10. Answer not provided - See Critique Sheet
11. A
12. A
13. A
14. A
15. A (Multiple booths not utilized)
16. B
17. Answer not provided - See Critique Sheet
18. A
19.
20. A
21. B
22. A
23. A
24. Detector does not have doors
25. A (Only one booth)
26. A
27. A

TAMPER INDICATING CIRCUITS

ANSWERS

1. A
2. D
3. A or B
4. A
5. A
6. A
7. D

NOTE: These are generic answers. Obviously, the ETQ is answered specifically for each component utilizing tamper circuitry protection.

TAMPER SEAL AND INSPECTION

ANSWERS

1. A
2. A
3. A
4. B
5. Not applicable
6. Not applicable
7. C
8. A
9. C

VAULTS

ANSWERS

1. A
2. D & E
3. F
4. 1.5 minutes
5. Below grade
6. A
7. B
8. A
9. A

PACKAGE SEARCH - VISUAL INSPECTION

ANSWERS

1. Answer not provided; some will have tamper seals, all others are opened.
2. A
3. A
4. A
5. A
6. A
7. A
8. A
9. Answer not provided; some will have tamper seals, all others are opened.
10. A
11. A
12. B (See Critique Sheet)
13. D
14. A

WEAPONS DETECTOR HAND-HELD, PACKAGE SEARCH

ANSWERS

1. A
2. A
3. A
4. A
5. A
6. A
7. B - See Critique Sheet
8. A
9. A
10. B
11. A
12. A
13. A

WEAPONS DETECTOR - WALK THROUGH

ANSWERS

1. A
2. A
3. A
4. A
5. A
6. A
7. C
8. A
9. A
10. B
11. B
12. A
13. A
14. A
15. A
16. B
17. A
18. B
19. A
20. A
21. B
22. A
23. B
24. A
25. A
26. A
27. A
28. A
29. A

6.0 DESIGN GUIDANCE COMPENDIUM CRITIQUE

The critique of the Design Guidance Compendium is segregated into two parts. Part I encompasses an overview of the completeness, validity, and utility of the Design Guidance Compendium with respect to its ability to aid the licensee in designing a Physical Protection System and in preparing the associated license document; the Physical Protection Plan. Part II of the critique focuses on individual components of the Design Guidance Compendium.

6.1 Overview Critique of the Design Guidance Compendium

The Design Guidance Compendium encompasses an extensive and inclusive collection of guidance, regulatory requirement interpretations, and design methodology documents. This information is invaluable to the fixed nuclear facility licensee in designing a Physical Protection System and in preparing and documenting a Physical Protection Plan which complies with the Physical Protection Upgrade Rule. The principal body of information contained within the Design Guidance Compendium is the Standard Format and Content Guide. This section solicits, in a precise and accurate manner, the types and levels of information which are required by the NRC's licensing process. The methodology utilized to solicit the information is easily comprehended, results in a well-structured license document, and minimizes the probability of an incomplete plan being submitted or of information being submitted which is not relevant to evaluating the degree of compliance exhibited by the Physical Protection Plan. Consequently, the licensing process becomes more standardized and less burdensome. In addition to aiding the preparation and documentation of an acceptable plan, the Standard Format and Content Guide facilitates and enhances the licensee's efforts to design the total Physical Protection System. These attributes result from the inherent capability of the Standard Format and Content Guide to expose the licensee to a continuous evaluation of the Physical Protection System's performance capabilities. Resultantly, component inadequacies and system incongruencies are continuously identified during the course of preparing the license document and designing the Physical Protection System.

The Intent and Scope of the Regulations is another body of information contained within the Design Guidance Compendium. This section is helpful in assisting the licensee to accurately interpret the regulatory requirements specified in the Physical Protection Upgrade Rule. The utilization of questions and answers is a positive approach to both clarifying the meaning of the requirement and in justifying its presence as a regulatory requirement. For those organizations which are entering the nuclear field or who have not been exposed to the licensing process, this body of regulatory interpretations and information is essential. Additionally, the benefits derived from the tables which identify and cross-reference information and requirements contained in 10 CFR 73.45 and 10 CFR 73.46 are invaluable.

The third body of information, the Design Methodology Document section, is comprised of three parts. The first, the Logic Trees, depicts the integration of the various regulatory requirements into the total performance capability. This section is useful in defining the broad picture of the performance capability. Part II, the Component Matrices, identifies those safeguard measures, components, and systems which are available to the licensee pursuant to designing a Physical Protection System.

This section is beneficial to new licensees, who do not have ready access to current safeguards technology, in the component selection process. Part III, the Effectiveness Test Questionnaires (ETQ), provides the licensee with a range of graded performance levels which can be achieved by each component. This section is extremely helpful and is responsive to the needs of the licensee to evaluate the effectiveness of the Physical Protection System in complying with the performance capabilities. Consequently, as components are added to the Physical Protection System, the licensee is afforded the opportunity to compensate for minimal performance in one area by elevating the performance levels of another component or system within the same physical protection subsystem. This attribute is most beneficial to those facilities which, by design, are limited to specific physical protection applications.

The Bibliography and Microfiche Library is the last body of information contained in the Design Guidance Compendium. This section, which consists of an exhaustive and reliable source of technical information, is useful to the licensee by referencing a wealth of information which can be utilized in designing the Physical Protection System.

6.2 Specific Component Critique

This section critiques the Design Guidance Compendium by focusing upon particular compendium components, specifically, the performance capability developmental guidance of Chapter 18, the compendium's Sample Plan, and each Information Request Sheet (IRS) and its associated Effectiveness Test Questionnair (ETQ).

6.2.1 Performance Capability Developmental Guidance (Chapter 18)

Chapter 18's content is inclusive and the guidance facilitates the development of a well-structured physical protection plan. Information is solicited in a clear and, usually, concise manner and the guidance is easily comprehended. In short, the developmental guidance provides the licensee with sufficient direction to prepare and submit an acceptable physical protection plan.

6.2.2 Sample Plan

The sample plan was not critiqued with the same intensity as the remainder of the Design Guidance Compendium. Instead, the sample plan was viewed solely as an instrument to aid the licensee in understanding the level of information required by the NRC and in formulating the plan's organization. In these respects, the sample plan is adequate.

6.2.3 Information Request Sheets/Effectiveness Test Questionnaires

The critique of the IRS and ETQ forms is conducted in two parts. The first presents an overview of the "value" of the forms, respective of their current condition. "Value" is defined as the ability to support the licensee's efforts to provide the NRC with an acceptable level of detailed technical information. The second part of the critique is comprised of critique sheets for each ETQ and IRS completed. The critique sheets identify weak areas in each form and provide ideas for increasing their "value."

6.2.3.1 Overview of the IRS and ETQ Forms

The NRC's evaluation of the plan's effectiveness and acceptability focuses on the plan's ability to satisfy generic developmental criteria and the performance capability requirements established by the Safeguards Upgrade Rule. The maximum "value," associated with the IRS and ETQ forms, exists only when the information solicited by an IRS form is evaluated by an associated ETQ and when only information worthy of evaluation is solicited. At present, a direct correlation between the IRS and ETQ forms does not exist. Figure 6.1 graphically depicts the following variations in IRS and ETQ correlations:

- Example "A" indicates a situation where not all of the information solicited is evaluated and where information is evaluated, but not requested.
- Example "B" indicates a situation where more information is solicited than evaluated.
- Example "C" indicates a situation where more information is evaluated than solicited.

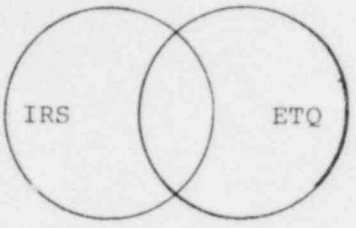
The problems associated with and contributed by the lack of correlation between the information requested and the information evaluated appears to be the most notable deficiency with the IRS/ETQ Forms. A correlation equating one, between the information requested and evaluated, is not possible or practical. For example, the function of a component and a generic system description cannot be evaluated. However, this information is worthy of solicitation. The remainder of pertinent information; e.g., performance criteria, maintenance and testing, detection and assessment, and vulnerabilities, is capable of being evaluated. Two solutions are available. First, the IRS and ETQ Forms could be incorporated into one questionnaire. A second solution, which allows the IRS and ETQ Forms to remain separate, involves a reexamination of both the information requested and the information evaluated. The principal concern being the development of consistency between the requested and evaluated information. Both of these alternatives allow the NRC to propose

definitive questions applicable to evaluating the performance capability of each system, component, and procedure. Additionally, the licensee is afforded the opportunity to evaluate each specific response and the composite effectiveness of his Physical Protection Plan based on the graded performance level answers. Figure 6.2 illustrates a standard organizational format which could be utilized by either solution to provide the necessary information. Whichever solution is adopted, the effort undertaken to achieve this correlation, to develop consistency between the information requested and that evaluated, will significantly enhance the completeness, validity, and utility of the Design Guidance Compendium.

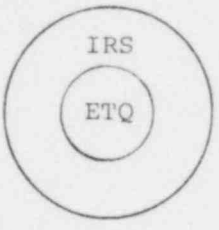
FIGURE 6.1

CORRELATION BETWEEN INFORMATION REQUEST SHEETS AND EFFECTIVENESS TEST QUESTIONNAIRES

A.



B.



C.

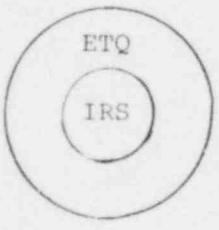


FIGURE 6.2

STANDARD ORGANIZATIONAL FORMAT

I. FUNCTION

II. SYSTEM DESCRIPTION

III. PERFORMANCE CRITERIA

- A. Site Conditions
- B. Environmental Conditions
  1. Natural
  2. Man-made
- C. Performance Conditions
  1. Installation/Placement
  2. Construction
  3. Operation
     - a. Closed Portal
     - b. Open Portal
  4. Penetration Times
  5. Reliability
  6. Protective Features
  7. Diversity and Redundancy
  8. Operator Training
  9. System Interfaces
  10. Power Supplies
  11. Accountability
  12. Design Criteria
  13. Calibration
  14. Performance Testing
  15. Response
      - a. Active Adversary Action
      - b. Passive Adversary Action

IV. MAINTENANCE AND TESTING

- A. Maintenance
  1. Corrective Maintenance
  2. Preventative Maintenance

FIGURE 6.2 (CONTINUED)

STANDARD ORGANIZATIONAL FORMAT

B. Testing

1. Operational Checks
2. Testing Frequencies
3. Who Performs the Test
4. How is the Test Performed

V. DETECTION AND ASSESSMENT

A. Detection

1. Type of Detectors
2. Local/Remote Alarms

B. Assessment

1. Methods of Assessment

a. Local Assessment
b. Remote Assessment

2. Who Performs Assessment

VI. VULNERABILITIES

6.2.3.2 Critique Sheets

The following critique sheets are arranged according to IRS and ETQ reference numbers.

ADMITTANCE AUTHORIZATION CRITERIA AND SCHEDULES

I. INFORMATION REQUEST SHEETS (Revised 10/5/79)

A. The IRS Form does not utilize definitive questions.

B. Question No. 3 - Identity verification should be part of "Admittance Authorization/Verification Procedures."

C. Request information concerning systems which utilize criteria other than authorization papers.

D. Request information on how schedules are maintained.

E. Reorganize to obtain a more structured format.

F. The IRS Form is a good indicator of the types of information which should be requested.

II. EFFECTIVENESS TEST QUESTIONNAIRE

A. Correlation is lacking between the information requested by the IRS Form and the information evaluated by the ETQ Form. This constitutes a major and unresolved problem.

B. The ETQ does not evaluate how the schedules are maintained.

C. The ETQ does not evaluate auditing measures.

D. The ETQ does not evaluate vulnerabilities.

E. ETQ should evaluate the admittance authorization criteria against a standard.

REFERENCE 2-1
CRITIQUE SHEET

ADMITTANCE AUTHORIZATION VERIFICATION PROCEDURES

I. INFORMATION REQUEST SHEET (Revised 9/5/79)

A. Correlation is lacking between information requested by the IRS Forms and the information evaluated by the ETQ Forms. This constitutes a major and unresolved problem.

B. Information requests are not presented in definitive form.

C. The IRS Form adequately requests information concerning a paper-oriented authorization verification system. However, because the example system is computerized, most of the requested information is contained in the "Admittance Authorization Criteria and Schedules" IRS Form. Provisions should be made for an advanced verification system.

II. EFFECTIVENESS TEST QUESTIONNAIRES

A. Generally, the ETQ Form does not evaluate an automated verification process. Questions No. 2, 3, 4, 6, 9, 10, 12, and 13 are not applicable to the computerized system.

B. If the ETQ is intended to evaluate a paper-oriented verification system, the following should be evaluated:

1. Training of personnel utilizing written procedures
2. Auditing records
3. Maintenance of records
4. Elevated levels of admittance authorization.

There is considerable inconsistency between the IRS Form and the ETQ Form.

C. Question No. 11 - What if the visitor's employer does not have a security organization? What if the visitor is a U. S. Senator? Flexibility should be built into this question. For some visitors, calling the employer for a physical description is warranted. Using schedules for visitors is also a good idea.

AIR AND UTILITY INLET BARRIERS

I. INFORMATION REQUEST SHEETS

1. The licensee should be provided with an IRS which requests information concerning air and utility penetrations in the physical barrier which are not protected by an inlet barrier. In some cases, the design and placement of the inlets may enhance the security of the MAA and vault to a greater extent that the inlet barrier.

2. Reorganize to obtain a more structured format.

3. The IRS Form should utilize definitive questions.

4. Request information concerning detection and assessment of an adversary action.

5. If the detection system possesses alarms, the IRS should request where and how they annunciate.

II. EFFECTIVENESS TEST QUESTIONNAIRES

1. Evaluate detection and assessment measures.

2. Evaluate alarm annuciations, if utilized.

3. See I.1 above.

BALANCED MAGNETIC SWITCHES

I. INFORMATION REQUEST SHEETS

A. Reorganize to obtain a more structured format.

B. Utilize only definitive questions. Paragraph No. 4 is a good example of a definitive question.

C. Vulnerability information is not requested.

D. Environmental conditions, which are pertinent to the operation of the magnetic switch, are not requested.

II. EFFECTIVENESS TEST QUESTIONNAIRE

A. ETQ does not evaluate local/remote alarm annunciation.

B. Questions No. 1 and No. 2 are more pertinent to the construction of the door.

C. The ETQ does not evaluate information concerning who performs the tests and maintenance.

CCTV MONITORING/SURVEILLANCE

I. INFORMATION REQUEST SHEETS

A. Questions No. 2, 3, 4, and 5 are a repetition of the information requested in IRS Form 11-1. Much of the information requested in Question No. 1 is also repetitious.

B. Information requested is not consistent with the information evaluated by the ETQ Form.

C. Only the third sentence of Question No. 1 and Question No. 6 are applicable to surveillance and assessment.

II. EFFECTIVENESS TEST QUESTIONNAIRE

A. Questions No. 13, 14, and 15 are a repetition of the information evaluated in ETQ Form 11-1.

B. The operations section of the ETQ Form is a good representation of the types of information which should be requested and evaluated.

C. Answer No. 6 should have an answer pertaining to continuous coverage as part of answer "A."

REFERENCE 11-1
CRITIQUE SHEET

CCTV SYSTEMS

I. INFORMATION REQUEST SHEETS

A. The IRS form was very well structured.

B. A good representation of the types of information which should be requested.

II. EFFECTIVENESS TEST QUESTIONNAIRE

A. ETQ should include detection and assessment evaluations.

B. Question No. 7 -- Rephrase so that it is applicable to interior areas.

C. ETQ does not evaluate video recording devices.

CODED CREDENTIAL SYSTEM

I. INFORMATION REQUEST SHEETS

A. Reorganize to obtain a more structured format.

B. The IRS Form should utilize definitive questions.

C. Request information concerning how often the system is tested and who performs the test.

D. Request information concerning detection and assessment of false credentials.

II. EFFECTIVENESS TEST QUESTIONNAIRES

A. Does not evaluate tests utilizing false credentials: e.g., who conducts the tests and at what frequency.

CONTROLLED SECURITY LIGHTING

I. INFORMATION REQUEST SHEETS (Revised 9/5/79)

A. The exact location of the lighting system components is not as important as the illumination provided by the controlled security lighting system over the area of coverage. It may be unnecessary to solicit a map identifying the location of the lamps.

B. The IRS Form is a representative sample of the types of information which should be requested to adequately describe the controlled security lighting system.

II. EFFECTIVENESS TEST QUESTIONNAIRE

A. Questions No. 1 and No. 3 deal with exterior lighting. The questions should be worded in a manner which excludes them from the questionnaire if the lighting system is interior. Answer No. 3 - for exterior lighting, answer 3.d should be part of answer 3.a.

B. Question No. 10 - Instead of a YES or NO, answers could be graded on the basis of whether all of the lighting components are located inside a PA, a VA, or an MAA.

C. The ETQ Form is a representative sample of the types of information which should be evaluated to adequately describe the controlled lighting system.

DOORS AND ASSOCIATED HARDWARE

I. INFORMATION REQUEST SHEETS

A. Reorganize to obtain a more structured format.

B. The IRS Form should utilize definitive questions.

C. Request information concerning who tests alarms, the testing frequency, where the alarms annunciate, type of annunciation, and the maintenance schedules for alarms.

D. Request information concerning who assesses an alarm and from where.

E. The most important characteristic of a door is its penetration time. Information concerning construction, materials used, etc., should only be requested as necessary to support the penetration delay times.

F. Vulnerabilities are not requested.

II. EFFECTIVENESS TEST QUESTIONNAIRE

A. No maintenance or testing questions are evaluated.

B. The ETQ does not evaluate information concerning features which could compromise penetration delay times.

C. The ETQ does not evaluate information pertinent to detection, assessment, or response activities.

D. Question No. 1 does not evaluate the situation where one type of door is used as both a MAA and vault door. The door does not become more secure because it is a barrier to the vault.

E. Question No. 3 should have as its best answer. "No Vehicle Door Installed."

F. Question No. 9 - Adversary tools may include tools from more than one performance level. Example, the door may be explosives while the locking mechanism may be thermal devices.

REFERENCE 22-1
CRITIQUE SHEET

DURESS ALARMS

I. INFORMATION REQUEST SHEETS (Revised 10/5/79)

A. Correlation is lacking between information requested by the IRS Forms and the information evaluated by the ETQ Forms. This constitutes a major and unresolved problem.

B. The IRS questions are not presented in a definitive manner.

II. EFFECTIVENESS TEST QUESTIONNAIRES

A. Question No. 3 - Answer A and B should read to the effect: . . .activated microphones and/or CCTV cameras providing audio and/or visual coverage of vital points/areas.

B. The ETQ Form evaluates only voluntary types of duress alarms. Nonvoluntary types of duress alarms, such as those which monitor physiological conditions, should also be evaluated.

EMERGENCY EXITS

I. INFORMATION REQUEST SHEETS

A. Reorganize to obtain a more structured format.

B. The IRS should utilize definitive questions.

C. No maintenance-related questions are requested.

D. Vulnerabilities are not requested.

E. Request information concerning who tests the alarms.

F. The most important characteristic of a door is its penetration time. Information concerning construction, material used, etc., should only be requested as necessary to support the penetration delay times.

II. EFFECTIVENESS TEST QUESTIONNAIRE

A. Depending upon the penetration times of the emergency exit, redundant barriers and/or diverse materials may not be required. The performance level answers (YES or NO) do not evaluate this option.

B. No maintenance-related questions evaluated.

C. Answer No. 11 does not correspond to question No. 11.

D. Answer No. 13 - Door may not require tamper seals. The doors described for the hypothetical facility would not require seals.

EQUIPMENT CHECKS/MAINTENANCE

I. INFORMATION REQUEST SHEETS (Revised 9/5/79)

A. The information requested by the IRS is inconsistent with the information evaluated by the ETQ Form. The IRS Form should request, generically, all of the information evaluated by the ETQ Form.

B. Questions in this IRS Form are definitive.

II. EFFECTIVENESS TESTS QUESTIONNAIRE

A. Include an evaluation of personnel training to perform the equipment checks/maintenance procedure.

B. Overall, the ETQ Form is a good representation of the type of information which should be evaluated.

ESCORTS

I. INFORMATION REQUEST SHEETS

A. Reorganize to obtain a more structured format.

B. The IRS Form should utilize definitive questions.

C. Request information about how the initial identification of the individual is obtained. He is potentially the most threatening, not the escort or another individual inside the facility.

II. EFFECTIVENESS TEST QUESTIONNAIRES

A. Question No. 4 - Does not evaluate the situation where an escort cannot transfer responsibilities.

B. Question No. 7 - Answer A.1, having a visitor being escorted by his internal contact is a very likely example of collusion. The answers should be reevaluated.

C. Question NO. 8 - The "Sample Plan" indicates that entry control personnel are not armed. The questionnaire indicates that arming escorts is preferred. Consistency is needed.

EXPLOSIVE DETECTOR HAND-HELD, PACKAGE SEARCH

I. INFORMATION REQUEST SHEETS (Revised 10/5/79)

A. Correlation is lacking between information requested by the IRS Forms and the information evaluated by the ETQ Forms. This constitutes a major and unresolved problem.

B. Operator training information is not requested.

C. The revised edition of IRS Forms is less effective in requesting information relative to evaluating a component or procedure than the prior IRS edition. Questions are not presented in a definitive manner.

II. EFFECTIVENESS TEST QUESTIONNAIRE

A. The ETQ is an effective evaluation of the methodology for utilizing an explosive detector while conducting a package search.

EXPLOSIVE DETECTOR HAND-HELD, PERSONNEL SEARCH

I. INFORMATION REQUEST SHEETS (Revised 10/5/79)

A. Correlation is lacking between information requested by the IRS Forms and the information evaluated by the ETQ Forms. This constitutes a major and unresolved problem.

B. Operator training information is not requested.

C. The revised edition of IRS Forms is less effective in requesting information relative to evaluating a component or procedure than the prior IRS edition. Questions are not presented in a definitive manner.

II. EFFECTIVENESS TEST QUESTIONNAIRE

A. Question No. 2 - Indicates that long lines which will result in expediting the search are preferred. Answer A should be "NO" and Answer B should be "YES."

B. Does not evaluate any information concerning the calibration of the explosives detector. See Question No. 8 for "Explosive Detector Hand-Held, Package Search."

C. Questions No. 8 and No. 9 should be deleted as they are applicable to ETQ No. 32.

FLOORS, ROOFS, WALLS

I. INFORMATION REQUEST SHEETS

A. Reorganize to obtain a more structured format.

B. Utilize only definitive questions. Paragraph No. 3 is a good example of a definitive question.

C. The most important characteristic of a physical barrier is its penetration time. Information concerning construction, materials utilized, etc., should only be requested as necessary to support the penetration delay times.

D. There is only one IRS form for the three types of physical barriers. Three separate ETQ forms are used for each type of physical barrier. Initially, this is a little confusing.

II. EFFECTIVENESS TEST QUESTIONNAIRES

A. Wall, Floor, and Roof ETQ's.

1. These ETQ's do not evaluate any questions pertinent to detection, assessment, or response activities.

2. Depending upon the penetration times of the physical barriers, redundant barriers and/or diverse materials may not be required. The performance level answers (YES or NO) do not evaluate this option.

B. Wall ETQ

1. This ETQ does not evaluate information concerning features which could compromise penetration delay times.

C. Floor ETQ

1. Floors can also be below grade. The performance level answers do not evaluate this option.

LOCAL AUDIBLE/VISIBLE ALARMS

I. INFORMATION REQUEST SHEETS

A. Question No. 1 - The sensitivity, reliability, probability of detection, and false alarm rate of the sensor should be part of the sensor's IRS Form.

B. The IRS Form is a good representation of the types of information which should be requested.

II. EFFECTIVENESS TEST QUESTIONNAIRES

A. Questions No. 9 and No. 10 should be evaluated as part of the component or system ETQ Form.

MOTION DETECTORS - INTERIOR MICROWAVE SYSTEMS

I. INFORMATION REQUEST SHEETS (Revised 9/5/79)

A. The IRS Form was fairly well structured.

B. The IRS Form is a good representation of the types of information which should be requested.

II. EFFECTIVENESS TEST QUESTIONNAIRES

A. ETQ Form should include a detection and assessment evaluation.

B. Answer No. 6 - This answer should be modified for systems or components housed in a facility which is environmentally immune to lightning.

C. ETQ Form should include a redundant and diversity evaluation.

PHOTO IDENTIFICATION BADGE

I. INFORMATION REQUEST SHEETS

A. Reorganize to obtain a more structured format.

B. The IRS Form should utilize definitive questions.

C. Request information concerning tests utilizing false photo ID badges, how often the tests are conducted, and who conducts the tests.

II. EFFECTIVENESS TEST QUESTIONNAIRES

A. Question No. 12 should have a graded performance level rather than a YES or NO answer.

B. Questions No. 17 and 18 do not provide an answer for the situation when a comparison is not performed remotely.

POSITIVE PERSONNEL IDENTIFICATION

I. INFORMATION REQUEST SHEET

A. Reorganize to obtain a more structured format.

B. The IRS Form should utilize definitive questions.

C. The information requested sufficiently addresses the system's performance capabilities.

II. EFFECTIVENESS TEST QUESTIONNAIRE

A. Question No. 9 - Does not evaluate the situation where a reference file is not stored on the coded credential.

B. Question No. 10 - Does not evaluate the situation where the identifier system does not perform personnel accountability.

C. Question No. 14 - The Voice Verification System (VVS) tamper protection features are not evaluated by the questionnaire.

SECURED ACCESS PORTAL

I. INFORMATION REQUEST SHEETS

A. The secured access portal is really not a pedestrian sally port; however, the concepts were similar enough to allow use of the sally port IRS Form. In this respect, the sally port is a good representation of the information which should be requested.

II. EFFECTIVENESS TEST QUESTIONNAIRE

A. See I.A above. The ETQ Form is a good representation of the information which should be evaluated.

B. Answer 1.4 - Wood may not be allowed inside a facility because it is a fire hazard.

SHIELDING DETECTOR - WALK THROUGH

I. INFORMATION REQUEST SHEET (Revised 10/5/79)

A. Correlation is lacking between information requested by the IRS Forms and the information evaluated by the ETQ Forms. This constitutes a major and unresolved problem.

B. Operator training information is not requested.

C. Reorganize to obtain a more structured format.

D. The revised edition of the IRS Forms is less effective in requesting information relative to evaluating a component or procedure than the prior IRS edition. Questions are not presented in a definitive manner.

II. EFFECTIVENESS TEST QUESTIONNAIRE

A. Operator training, utilizing written procedures, is not evaluated.

B. Questions No. 1 and No. 4 indicate a confinement booth is required. Some detectors do not utilize a booth and audio communications are not required if the portal is manned and a nonbooth-type detector is employed.

C. Answer No. 7 should provide for the situation where an X-ray detector is not utilized in the MAA SAP for package searches.

D. Answer No. 10 should reflect the situation where a weight scale is not used.

E. Answer No. 15 should reflect the situation where multiple booths are not installed.

F. Question No. 16 - One percent, rather than 0.1%, appears to be sufficient for a false alarm rate. If not, the confidence rate should also be increased.

G. Question No. 24 - Answer should reflect the situation where the detector does not incorporate doors.

H. Question No. 25 - Answer should reflect situation where the MAA SAP does not have multiple booths.

I. ETQ should evaluate removing the individual to a remote search room if the cause of the alarm cannot be determined.

J. Since the weapons detector and the shielding detector are so similar, each of the respective ETQ Forms should be reviewed to ensure consistency of information evaluated by both forms.

TAMPER-INDICATING CIRCUITRY

I. INFORMATION REQUEST SHEETS

A. A very good representation of the type of information which should be requested.

B. IRS Form is well structured.

C. Questions are definitive.

II. EFFECTIVENESS TEST QUESTIONNAIRE

A. A very good representation of the type of information which should be evaluated.

B. The organizational structure of the ETQ Form should be revised.

TAMPER SEALS AND INSPECTIONS

I. INFORMATION REQUEST SHEET

A. Reorganize to obtain a more structured format.

B. Utilize only definitive questions.

C. Content inclusive

II. EFFECTIVENESS TEST QUESTIONNAIRE

A. Tamper seals are not always used just to ensure the integrity of SNM or waste containers. The questionnaire should be flexible enough to evaluate other tamper seal uses.

Two questionnaires, one soley for SNM and the other for variations in usage, may be more advantageous.

VAULTS

I. INFORMATION REQUEST SHEET

A. Some of the information requested requires completion of one or more of the other performance capabilities and Chapter 23 of the plan. Additionally, the majority of information, except as noted below, can be responded to by referencing other Information Request Sheets:

1. The purpose of the vault
2. Type and quantity of material stored
3. How the material is stored
4. Type of container
5. Frequency of access
6. Accessibility to exterior surfaces for inspection, assessment, and surveillance.

If the intent of the IRS Form is to provide an index of IRS Forms to facilitate an evaluation of the performance capabilities of the vault, it has achieved its purpose. If not, then only the above noted information should be requested.

B. Paragraphs No. 1 and 3 are very cumbersome. Reorganization is warranted.

II. EFFECTIVENESS TEST QUESTIONNAIRES

A. The ETQ Form is a fair representation of the types of information which should be evaluated.

PACKAGE SEARCH - VISUAL INSPECTION

I. INFORMATION REQUEST SHEET

A. The IRS Form is a good indicator of the types of information which should be requested.

B. The use of more definitive questions is applicable.

C. Information relative to testing is not requested.

D. Question No. 4 - Audit Methods. It is not necessary to have an audit for every search.

II. EFFECTIVENESS TEST QUESTIONNAIRE

A. Question No. 12 - The weapons and explosives ETQ's, identify a preference to remove the package to a remote area for inspection. In this ETQ, the package is not touched. Inconsistency exists.

B. The ETQ effectively evaluates information relative to a visual package search.

WEAPONS DETECTOR HAND-HELD, PACKAGE SEARCH

I. INFORMATION REQUEST SHEET (Revised 10/5/79)

A. A revised IRS Form covering this component was not included in the package. Resultantly, the IRS Form could not be evaluated.

II. EFFECTIVENESS TEST QUESTIONNAIRE

A. Operator training, utilizing written procedures is not evaluated.

B. Question No. 6 - How often is the calibration performed?

C. Answer No. 7 - Answer (A) should include, "All packages are opened."

D. Operator testing is not evaluated.

E. Answer No. 5 - should evaluate the r moval of the package to a remote search area.

F. The time spent implementing a search should be evaluated.

WEAPONS DETECTOR - WALK THROUGH

I. INFORMATION REQUEST SHEET (Revised 10/5/79)

A. Correlation is lacking between information requested by the IRS Forms and the information evaluated by the ETQ Forms. This constitutes a major and unresolved problem.

B. Operator training information is not requested.

C. Assessment information is not requested.

D. Questions are not presented in a definitive manner.

E. Reorganize to obtain a more structured format.

II. EFFECTIVENESS TEST QUESTIONNAIRE

A. Operator training, utilizing written procedures, is not evaluated.

B. Question No. 3 does not evaluate the situation where an X-ray conveyor is not in the area.

C. Question No. 7 is not applicable to manned portals when the entry control personnel ensure the individual passes through the detector.

D. Answer No. 9 should provide for using a hand-held weapons detector for carried articles.

E. Answer No. 10 should provide for the removal of the person to a remote search room if the cause of the alarm can not be located.

F. Answer No. 11 - Signal lights are rated higher than the security officer instructing the individual when to pass through the detector.

G. Question No. 18 - The throughput may not require multiple detectors. For an MAA, Answer B appears to be sufficient.

7.0 ADDITIONAL SUPPORT BEYOND THE SCOPE OF WORK

The contractual scope of work limited the development of the Physical Protection Plan to a MAA containing a single vault. The integration of those physical protection systems, which are exterior to the physical barriers of the MAA, with those inside the MAA or those portions of physical protection systems which extended beyond the physical barriers of the MAA was not addressed by the scope of this contract. Consequently, the evaluation process conducted by Sandia Laboratories and Woodward-Clyde Consultants was severely restricted. In a cooperative attempt to minimize this limitation and to facilitate and enhance the evaluation process, AGNS provided the following additional information:

(1) Answers to Effectiveness Test Questionnaires not addressed by the current scope of work.

(2) Matrices identifying the equipment and/or design features and procedures utilized to satisfy the performance capabilities.

7.1 Additional ETQ Form Answers

ANNUNCIATION SYSTEMS

ANSWERS

1. A
2. B
3. A
4. A
5. A
6. B
7. B
8. A
9. A
10. B
11. A
12. A
13. A
14. B
15. A
16. B
17. B

CENTRAL AND SECONDARY ALARM STATION

ANSWERS

1. A
2. B
3. A
4. A
5. A
6. A & B
7. A & B
8. A
9. A
10. A
11. A
12. B
13. B
14. B
15. A
16. A
17. A
18. A
19. A
20. A
21. A
22. A
23. A
24. A
25. B
26. A
27. A
28. A
29. A
30. A
31. A
32. A
33. A

CONTINGENCY PLAN

ANSWERS

1. A
2. A
3. A
4. A

EMERGENCY GENERATOR SYSTEMS

ANSWERS

1. A
2. A
3. A
4. A
5. Not Applicable
6. B
7. A
8. A
9. A
10. A
11. A
12. A

GUARD FORCE PATROLS/INTERVENTION

ANSWERS

1. A
2. A
3. A
4. A
5. A
6. A
7. A
8. A
9. A
10. A
11. A
12. N/A
13. A
14. A
15. A

INTERFACES (SENSOR - STATION)

ANSWERS

1. A
2. A
3. A
4. A
5. B
6. A
7. A
8. B
9. A
10. A

LOCKS

ANSWERS

1. A
2. D
3. A
4.
5.
6.
7.
8.
9.
10.
11.
12.
13.
14.
15.
16.
17.
18.
19.
20.
21.
22.
23.
24. B
25. A
26. A
27. A
28. A

PHYSICAL CONTROLS FOR KEYS, LOCKS, COMBINATIONS, AND CIPHER SYSTEMS

ANSWERS

1. A
2. A
3. A
4. A
5. A
6. A
7. A
8. A
9. A
10. A
11. B

HAND-HELD SNM DETECTOR - PACKAGE SEARCH

ANSWERS

1. A
2. A
3. A
4. A
5. A
6. A
7. All packages are opened
8. B - Tamper seals used
9. A
10. Answer not provided - prior to each open portal operation
11. A
12. A
13. A
14. A

HAND-HELD SNM DETECTOR - PERSONNEL SEARCH

ANSWERS

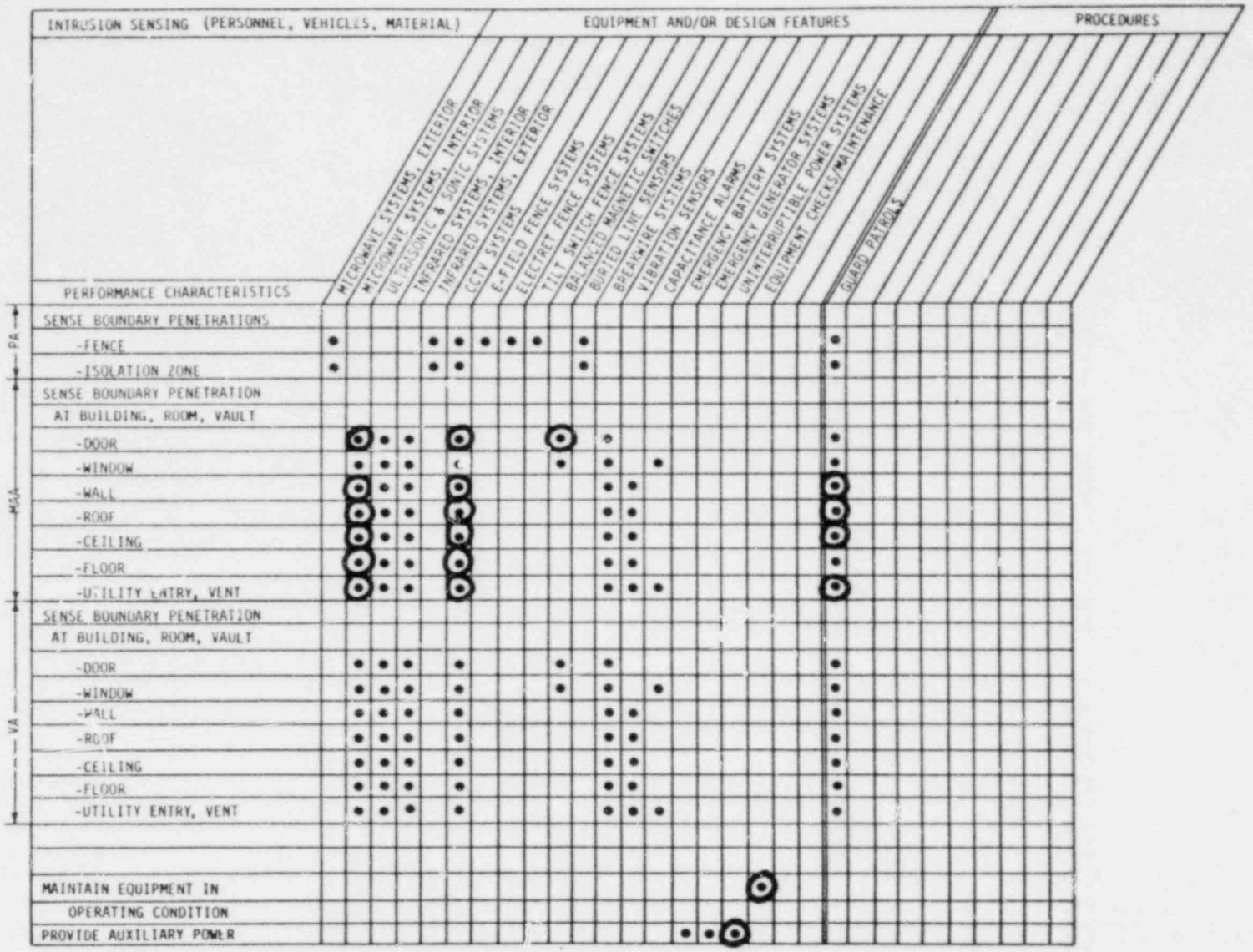
1. A
2. A
3. A
4. A
5. A
6. A
7. A
8. A
9. A
10. A
11. A
12. A
13. A
14. A
15. A
16. A
17. A

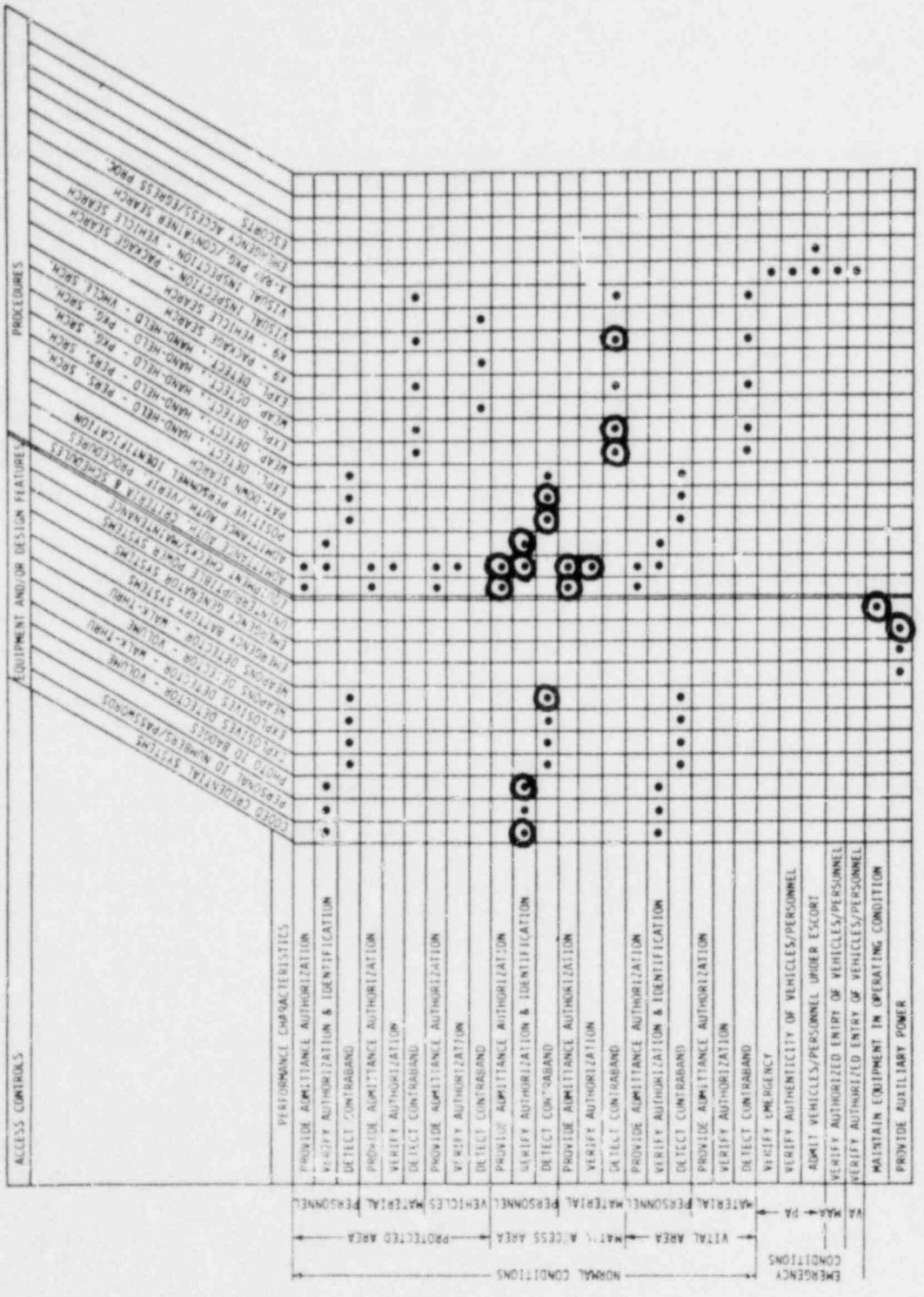
UNINTERRUPTIBLE POWER SYSTEM

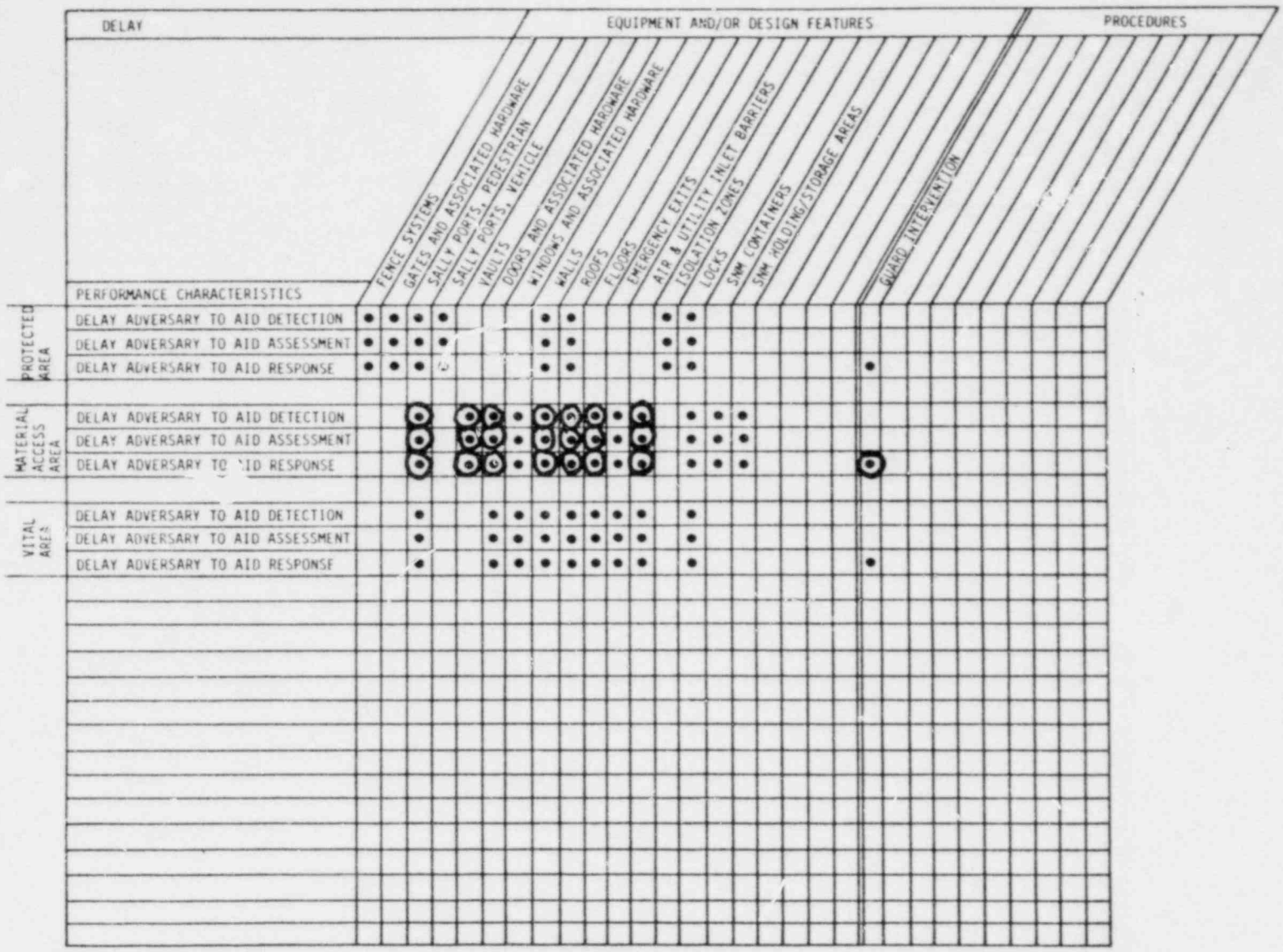
ANSWERS

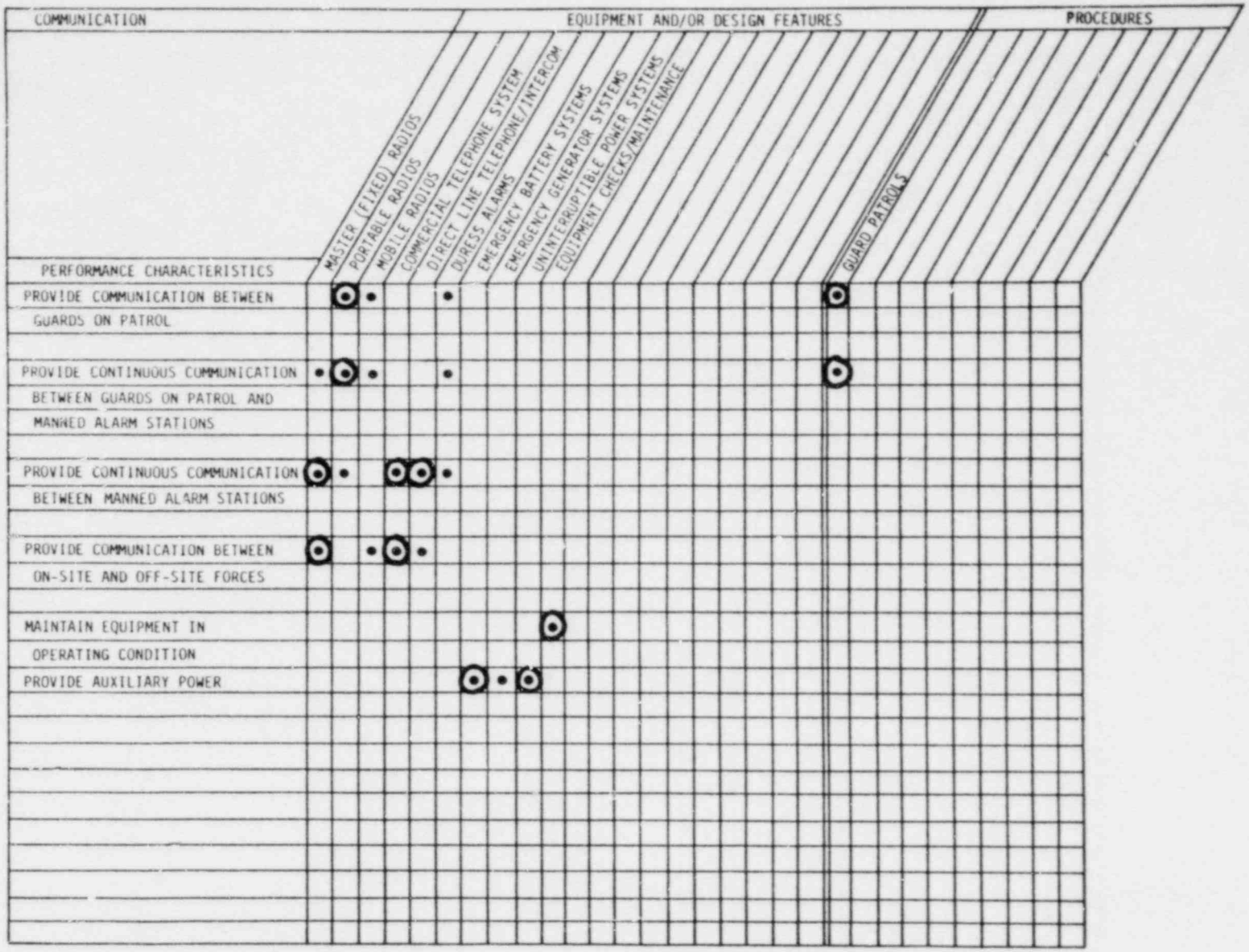
1. A
2. A
3. A
4. A
5. A
6. A
7. A
8. A
9. A
10. A
11. A
12. A
13. A
14. Question does not relate to answer.

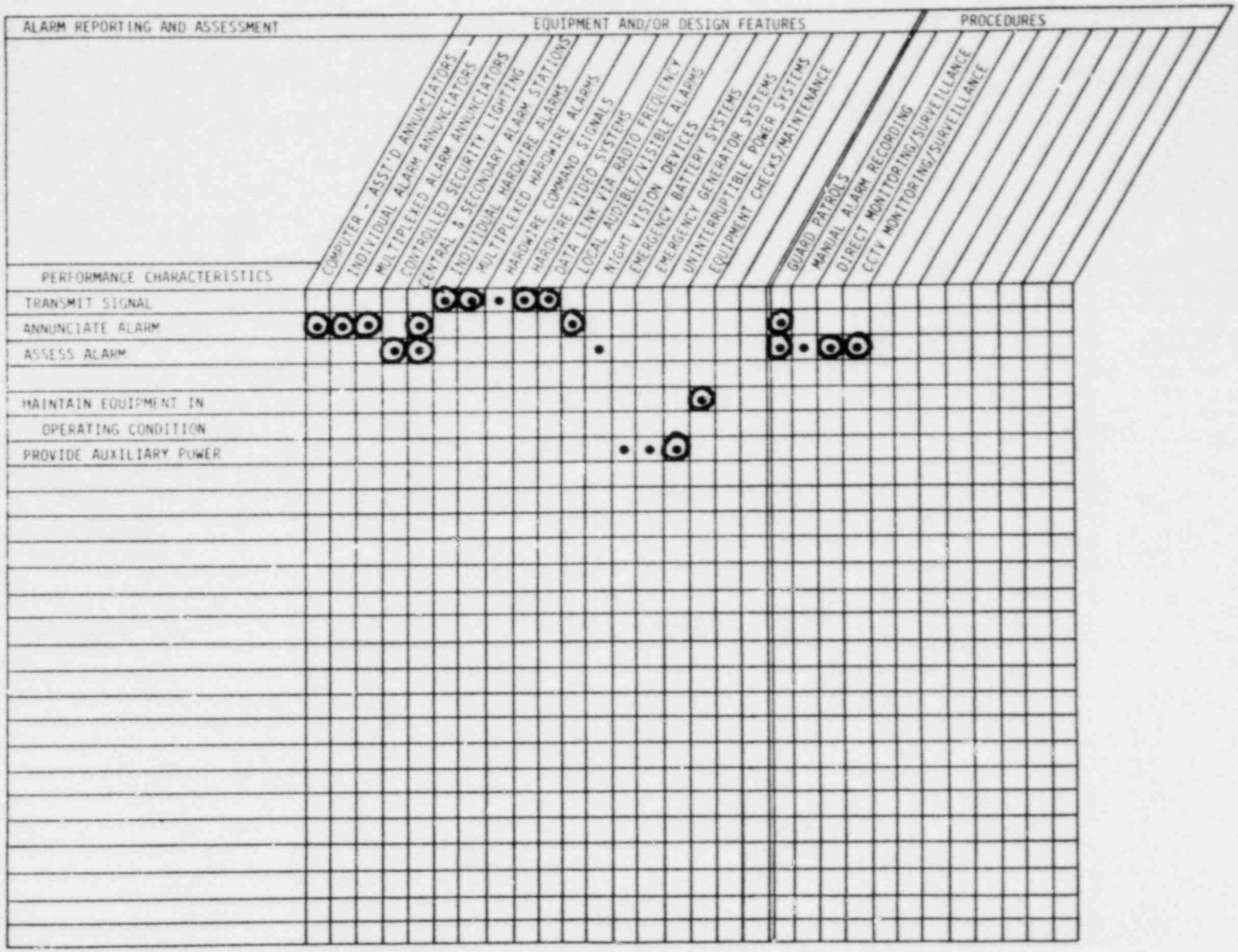
7.2 Matrices

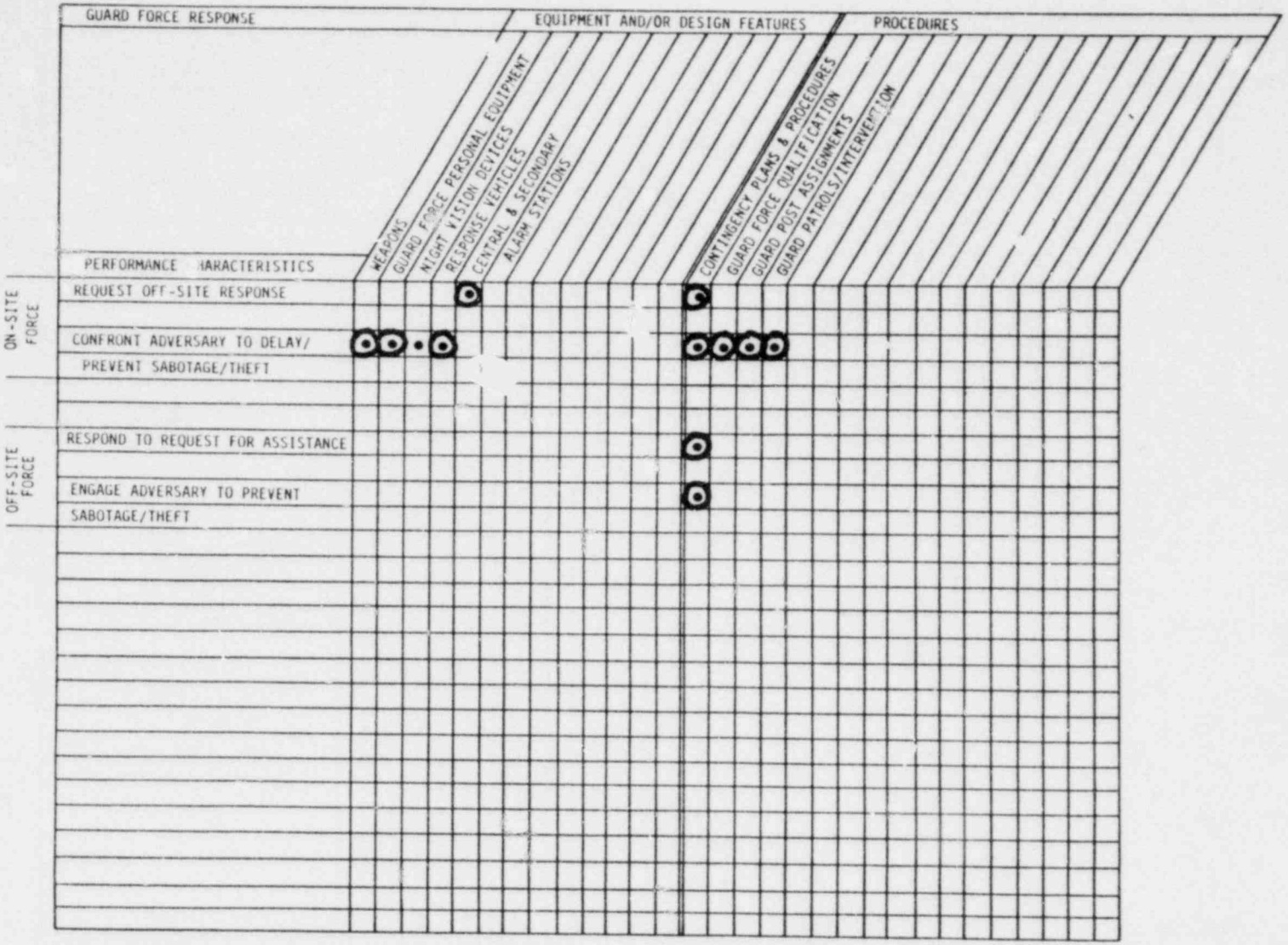

INTRUSION SENSING (PERSONNEL, VEHICLES, MATERIAL)
EQUIPMENT AND/OR DESIGN FEATURES
PROCEDURES
PERFORMANCE CHARACTERISTICS
MICROWAVE SYSTEMS, EXTERIOR
MICROWAVE SYSTEMS, INTERIOR
ULTRASONIC & SONIC SYSTEMS
INFRARED SYSTEMS, INTERIOR
INFRARED SYSTEMS, EXTERIOR
CCTV SYSTEMS
E-FIELD FENCE SYSTEMS
ELECTRET FENCE SYSTEMS
TILT SWITCH FENCE SYSTEMS
BALANCED MAGNETIC SWITCHES
BURIED MAGNETIC FENCE SYSTEMS
BREAKWIRE SYSTEMS
VIBRATION SYSTEMS
CAPACITANCE SENSORS
EMERGENCY ALARMS
EMERGENCY BATTERY SYSTEMS
UNINTERRUPTIBLE POWER SYSTEMS
EQUIPMENT GENERATOR SYSTEMS
EQUIPMENT CHECKS/MAINTENANCE
GUARD PATROLS
PA
MAA
VA
SENSE BOUNDARY PENETRATIONS
-FENCE
-ISOLATION ZONE
SENSE BOUNDARY PENETRATION
AT BUILDING, ROOM, VAULT
-DOOR
-WINDOW
-WALL
-ROOF
-CEILING
-FLOOR
-UTILITY ENTRY, VENT
SENSE BOUNDARY PENETRATION
AT BUILDING, ROOM, VAULT
-DOOR
-WINDOW
-WALL
-ROOF
-CEILING
-FLOOR
-UTILITY ENTRY, VENT
MAINTAIN EQUIPMENT IN
OPERATING CONDITION
PROVIDE AUXILIARY POWER

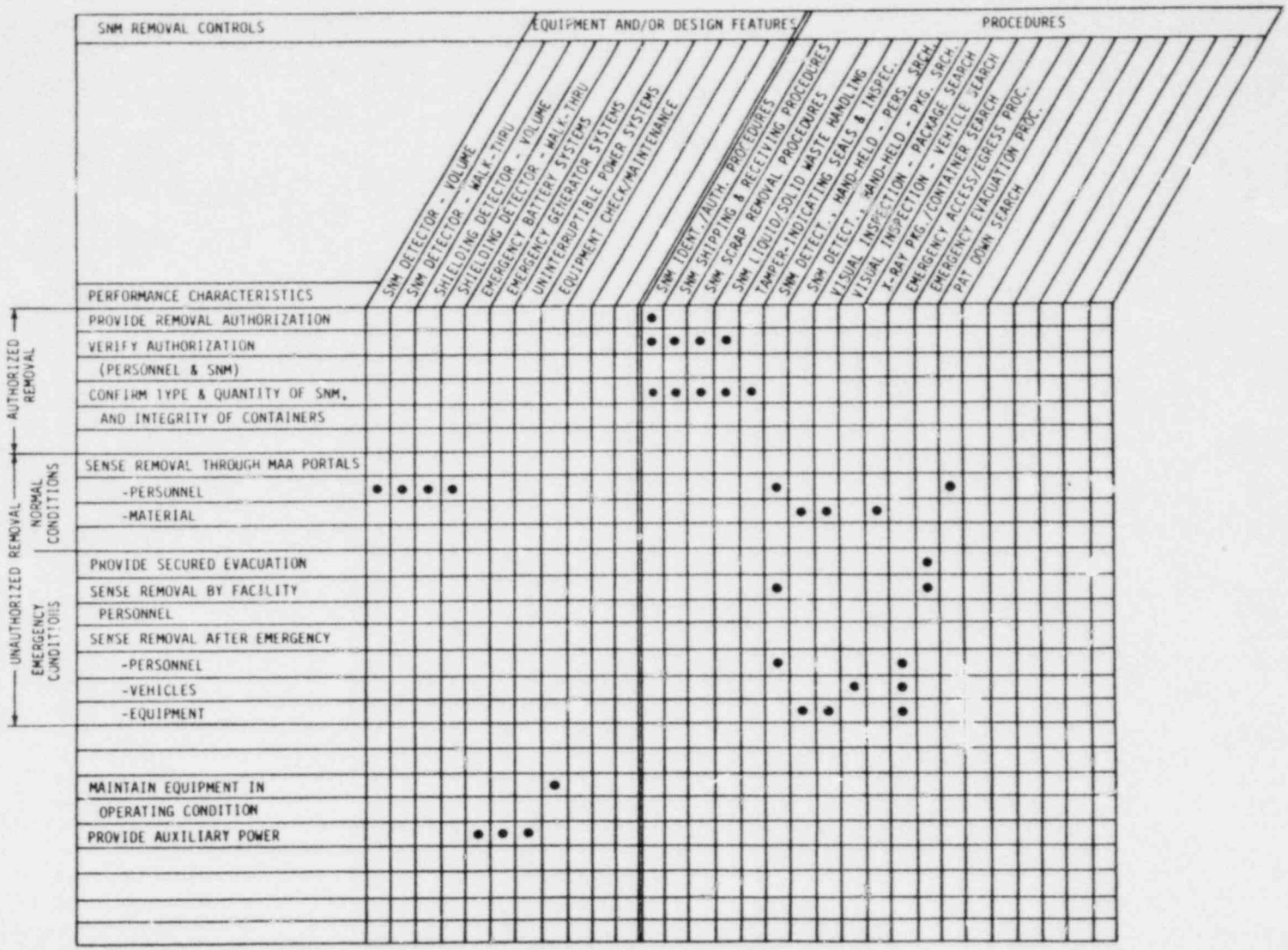

ACCESS CONTROLS
EQUIPMENT AND/OR DESIGN FEATURES
PROCEDURES
PERFORMANCE CHARACTERISTICS
PROVIDE ADMITTANCE AUTHORIZATION
VERIFY AUTHORIZATION & IDENTIFICATION
DETECT CONTRABAND
PROVIDE ADMITTANCE AUTHORIZATION
VERIFY AUTHORIZATION
DETECT CONTRABAND
PROVIDE ADMITTANCE AUTHORIZATION
VERIFY AUTHORIZATION
DETECT CONTRABAND
PROVIDE ADMITTANCE AUTHORIZATION
VERIFY AUTHORIZATION & IDENTIFICATION
DETECT CONTRABAND
PROVIDE ADMITTANCE AUTHORIZATION
VERIFY AUTHORIZATION
DETECT CONTRABAND
VERIFY EMERGENCY
VERIFY AUTHENTICITY OF VEHICLES/PERSONNEL
ADMIT VEHICLES/PERSONNEL UNDER ESCORT
VERIFY AUTHORIZED ENTRY OF VEHICLES/PERSONNEL
VERIFY AUTHORIZED ENTRY OF VEHICLES/PERSONNEL
MAINTAIN EQUIPMENT IN OPERATING CONDITION
PROVIDE AUXILIARY POWER
CODED CREDENTIAL SYSTEMS
PERSONAL ID BADGES
PHOTO ID BADGES/PASSWORDS
EXPLOSIVES DETECTOR - VOLUME
WEAPONS DETECTOR - WALK-THRU
WEAPONS DETECTOR - VOLUME
EMERGENCY BARRIER SYSTEMS - WALK-THRU
EMERGENCY GENERATOR SYSTEMS
EQUIPMENT CHECKS/MAINTENANCE
ADMITTANCE AUTH. CRITERIA & SCHEDULES
POSITIVE PERSONNEL IDENTIFICATION
PAT-DOWN SEARCH
EXPL. DETECT. - HAND-HELD - PERS. SRCH.
WEAP. DETECT. - HAND-HELD - PERS. SRCH.
EXPL. DETECT. - HAND-HELD - PERS. SRCH.
EXPL. DETECT. - HAND-HELD - PKG. SRCH.
K9 - PACKAGE SEARCH
K9 - VEHICLE SEARCH
VISUAL INSPECTION - PACKAGE SEARCH
VISUAL INSPECTION - VEHICLE SEARCH
X-RAY PKG. ICON. - VEHICLE SEARCH
EMERGENCY ACCESS/EGRESS PROC.
ESCORTS
NORMAL CONDITIONS
EMERGENCY CONDITIONS
PROTECTED AREA
MATL. ACCESS AREA
VITAL AREA
PERSONNEL
MATERIAL
VEHICLES
PERSONNEL
MATERIAL
PERSONNEL
MATERIAL
PA
MAA
VA

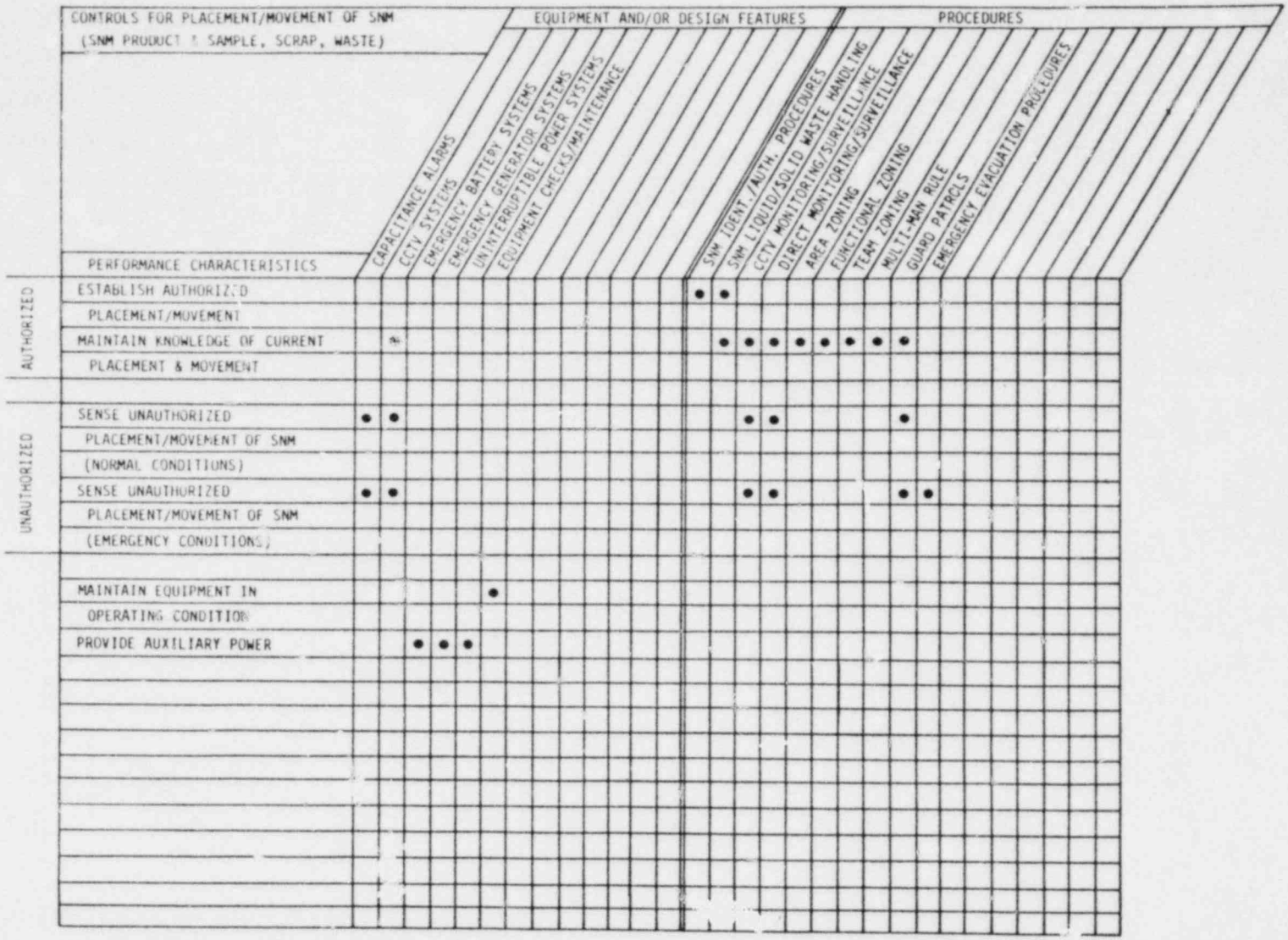

DELAY
EQUIPMENT AND/OR DESIGN FEATURES
PROCEDURES
PERFORMANCE CHARACTERISTICS
FENCE SYSTEMS
GATES AND ASSOCIATED HARDWARE
SALLY PORTS, PEDESTRIAN
SALLY PORTS, VEHICLE
VAULTS
DOORS AND ASSOCIATED HARDWARE
WINDOWS AND ASSOCIATED HARDWARE
WALLS
ROOFS
FLOORS
EMERGENCY EXITS
AIR & UTILITY INLET BARRIERS
ISOLATION ZONES
LOCKS
SNM CONTAINERS
SNM HOLDING/STORAGE AREAS
GUARD INTERVENTION
PROTECTED AREA
DELAY ADVERSARY TO AID DETECTION
DELAY ADVERSARY TO AID ASSESSMENT
DELAY ADVERSARY TO AID RESPONSE
MATERIAL ACCESS AREA
DELAY ADVERSARY TO AID DETECTION
DELAY ADVERSARY TO AID ASSESSMENT
DELAY ADVERSARY TO AID RESPONSE
VITAL AREA
DELAY ADVERSARY TO AID DETECTION
DELAY ADVERSARY TO AID ASSESSMENT
DELAY ADVERSARY TO AID RESPONSE


COMMUNICATION
EQUIPMENT AND/OR DESIGN FEATURES
PROCEDURES
PERFORMANCE CHARACTERISTICS
MASTER (FIXED) RADIOS
PORTABLE RADIOS
MOBILE RADIOS
COMMERCIAL TELEPHONE SYSTEM
DIRECT LINE TELEPHONE/INTERCOM
DURESS ALARMS
EMERGENCY BATTERY SYSTEMS
EMERGENCY GENERATOR SYSTEMS
UNINTERRUPTIBLE POWER SYSTEMS
EQUIPMENT CHECKS/MAINTENANCE
GUARD PATROLS
PROVIDE COMMUNICATION BETWEEN GUARDS ON PATROL
PROVIDE CONTINUOUS COMMUNICATION BETWEEN GUARDS ON PATROL AND MANNED ALARM STATIONS
PROVIDE CONTINUOUS COMMUNICATION BETWEEN MANNED ALARM STATIONS
PROVIDE COMMUNICATION BETWEEN ON-SITE AND OFF-SITE FORCES
MAINTAIN EQUIPMENT IN OPERATING CONDITION
PROVIDE AUXILIARY POWER

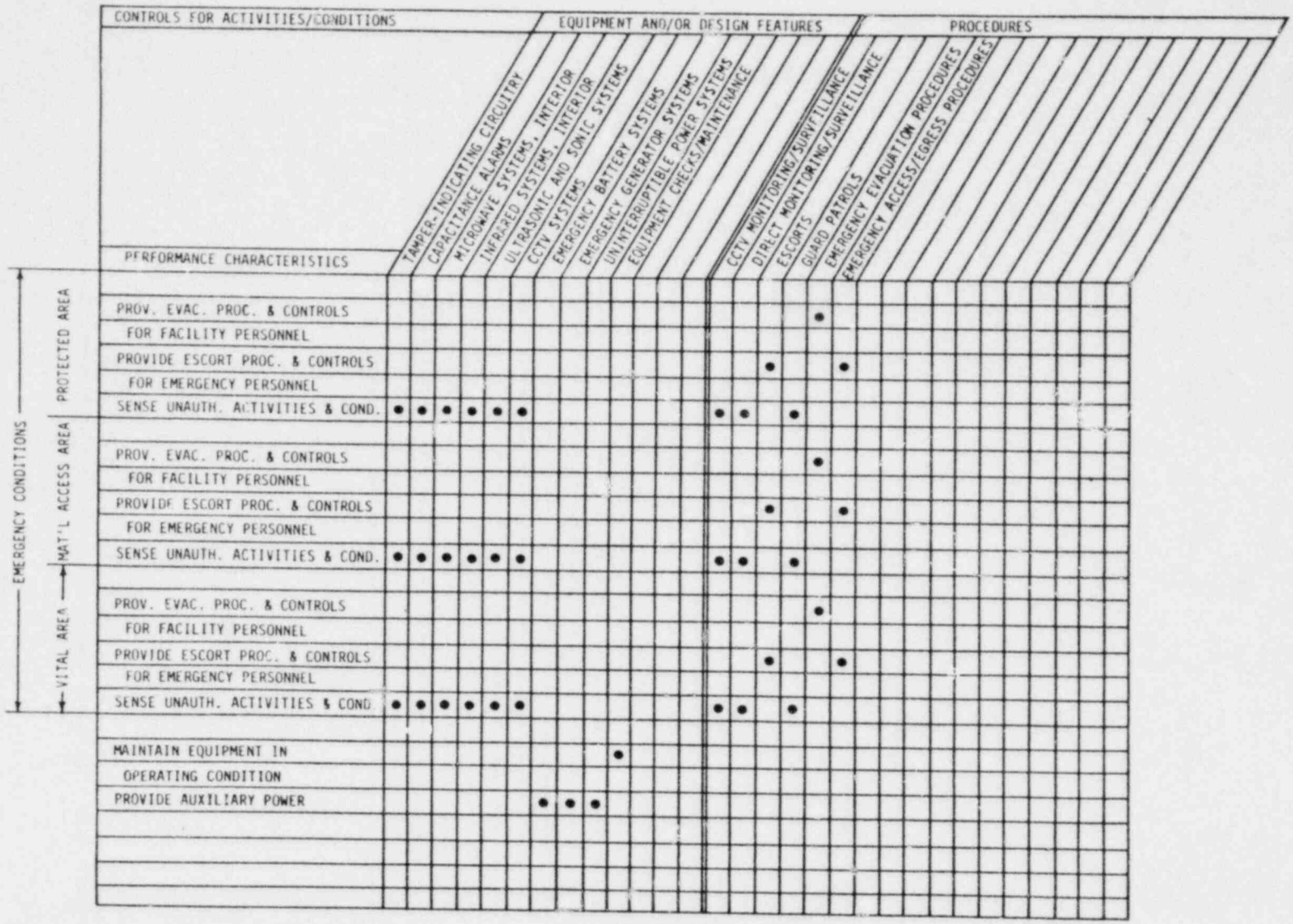

ALARM REPORTING AND ASSESSMENT
EQUIPMENT AND/OR DESIGN FEATURES
PROCEDURES
PERFORMANCE CHARACTERISTICS
TRANSMIT SIGNAL
ANNUNCIATE ALARM
ASSESS ALARM
MAINTAIN EQUIPMENT IN
OPERATING CONDITION
PROVIDE AUXILIARY POWER
COMPUTER - ASST'D ANNUNCIATORS
INDIVIDUAL ALARM ANNUNCIATORS
MULTIPLEXED ALARM ANNUNCIATORS
CONTROLLED SECURITY LIGHTING
CENTRAL & SECONDARY ALARM STATIONS
INDIVIDUAL HARDWIRE ALARMS
MULTIPLEXED HARDWIRE ALARMS
HARDWIRE COMMAND SIGNALS
DATA LINK VIA VIDEO SYSTEMS
LOCAL AUDIBLE/VISIBLE ALARMS
NIGHT VISION DEVICES
EMERGENCY BATTERY SYSTEMS
EMERGENCY GENERATOR SYSTEMS
UNINTERRUPTIBLE POWER SYSTEMS
EQUIPMENT CHECKS/MAINTENANCE
GUARD PATROLS
MANUAL ALARM RECORDING
DIRECT MONITORING/SURVEILLANCE
CCTV MONITORING/SURVEILLANCE


GUARD FORCE RESPONSE
EQUIPMENT AND/OR DESIGN FEATURES
PROCEDURES
WEAPONS
GUARD FORCE PERSONAL EQUIPMENT
NIGHT VISION DEVICES
RESPONSE VEHICLES
CENTRAL & SECONDARY ALARM STATIONS
CONTINGENCY PLANS & PROCEDURES
GUARD FORCE QUALIFICATION
GUARD POST ASSIGNMENTS
GUARD PATROLS/INTERVENTION
PERFORMANCE CHARACTERISTICS
ON-SITE FORCE
REQUEST OFF-SITE RESPONSE
CONFRONT ADVERSARY TO DELAY/ PREVENT SABOTAGE/THEFT
OFF-SITE FORCE
RESPOND TO REQUEST FOR ASSISTANCE
ENGAGE ADVERSARY TO PREVENT SABOTAGE/THEFT


SNM REMOVAL CONTROLS
EQUIPMENT AND/OR DESIGN FEATURES
PROCEDURES
PERFORMANCE CHARACTERISTICS
SNM DETECTOR - VOLUME
SNM DETECTOR - WALK-THRU
SHIELDING DETECTOR - VOLUME
SHIELDING DETECTOR - WALK-THRU
EMERGENCY BATTERY SYSTEMS
EMERGENCY GENERATOR SYSTEMS
UNINTERRUPTIBLE POWER SYSTEMS
EQUIPMENT CHECK/MAINTENANCE
SNM IDENT./AUTH. PROCEDURES
SNM SHIPPING & RECEIVING PROCEDURES
SNM SCRAP REMOVAL PROCEDURES
SNM LIQUID/SOLID WASTE HANDLING
TAMPER-INDICATING SEALS & INSPEC.
SNM DETECT.- HAND-HELD - PERS. SRCH.
VISUAL INSPECTION - HAND-HELD - PKG. SRCH.
VISUAL INSPECTION - PACKAGE SEARCH
X-RAY PKG./CONTAINER SEARCH
EMERGENCY ACCESS/EGRESS PROC.
EMERGENCY EVACUATION PROC.
PAT DOWN SEARCH
AUTHORIZED REMOVAL
PROVIDE REMOVAL AUTHORIZATION
VERIFY AUTHORIZATION
(PERSONNEL & SNM)
CONFIRM TYPE & QUANTITY OF SNM,
AND INTEGRITY OF CONTAINERS
UNAUTHORIZED REMOVAL
NORMAL CONDITIONS
SENSE REMOVAL THROUGH MAA PORTALS
-PERSONNEL
-MATERIAL
EMERGENCY CONDITIONS
PROVIDE SECURED EVACUATION
SENSE REMOVAL BY FACILITY
PERSONNEL
SENSE REMOVAL AFTER EMERGENCY
-PERSONNEL
-VEHICLES
-EQUIPMENT
MAINTAIN EQUIPMENT IN
OPERATING CONDITION
PROVIDE AUXILIARY POWER


CONTROLS FOR PLACEMENT/MOVEMENT OF SNM
(SNM PRODUCT & SAMPLE, SCRAP, WASTE)
EQUIPMENT AND/OR DESIGN FEATURES
PROCEDURES
CAPACITANCE ALARMS
CCTV SYSTEMS
EMERGENCY BATTERY SYSTEMS
EMERGENCY GENERATOR SYSTEMS
UNINTERRUPTIBLE POWER SYSTEMS
EQUIPMENT CHECKS/MAINTENANCE
SNM IDENT./AUTH. PROCEDURES
SNM LIQUID/SOLID WASTE HANDLING
CCTV MONITORING/SURVEILLANCE
DIRECT MONITORING/SURVEILLANCE
AREA ZONING
FUNCTIONAL ZONING
TEAM ZONING
MULTI-MAN RULE
GUARD PATROLS
EMERGENCY EVACUATION PROCEDURES
PERFORMANCE CHARACTERISTICS
AUTHORIZED
UNAUTHORIZED
ESTABLISH AUTHORIZED
PLACEMENT/MOVEMENT
MAINTAIN KNOWLEDGE OF CURRENT
PLACEMENT & MOVEMENT
SENSE UNAUTHORIZED
PLACEMENT/MOVEMENT OF SNM
(NORMAL CONDITIONS)
SENSE UNAUTHORIZED
PLACEMENT/MOVEMENT OF SNM
(EMERGENCY CONDITIONS)
MAINTAIN EQUIPMENT IN
OPERATING CONDITION
PROVIDE AUXILIARY POWER

	CONTROLS FOR ACTIVITIES/CONDITIONS	EQUIPMENT AND/OR DESIGN FEATURES													PROCEDURES																
	PERFORMANCE CHARACTERISTICS	TAMPER-INDICATING CIRCUITRY	CAPACITANCE ALARMS	MICROWAVE SYSTEMS, INTERIOR	INFRARED SYSTEMS, INTERIOR	ULTRASONIC AND SONIC SYSTEMS	CCTV SYSTEMS	EMERGENCY BATTERY SYSTEMS	EMERGENCY GENERATOR SYSTEMS	UNINTERRUPTIBLE POWER SYSTEMS	EQUIPMENT TESTS/MAINTENANCE				CCTV MONITORING/SURVEILLANCE	DIRECT MONITORING/SURVEILLANCE	AREA ZONING	FUNCTIONAL ZONING	TEAM ZONING	ESCORTS	PHYSICAL CONTROLS AND PROCEDURES	FOR LOCKS, KEYS, ETC.	CLOSE-OUT INSPECTIONS	MULTI-MAN RULE	GUARD PATROLS						
NORMAL CONDITIONS — PROTECTED AREA	ESTABL. AUTH. ACTIVITIES & COND.																●	●													
	PROVIDE SURVEILL. PROC. & CNTLS.						●								●	●	●	●	●					●	●						
	FOR FACILITY PERSONNEL																														
	PROVIDE ESCORT PROC. & CONTROLS																			●											
	FOR AUTHORIZED VISITORS																														
	SENSE UNAUTH. ACTIVITIES & COND.	●	●	●	●	●	●								●	●					●		●		●						
NORMAL CONDITIONS — MAT'L ACCESS AREA	ESTABL. AUTH. ACTIVITIES & COND.																●	●													
	PROVIDE SURVEILL. PROC. & CNTLS.						●								●	●	●	●	●					●	●						
	FOR FACILITY PERSONNEL																														
	PROVIDE ESCORT PROC. & CONTROLS																			●											
	FOR AUTHORIZED VISITORS																														
	SENSE UNAUTH. ACTIVITIES & COND.	●	●	●	●	●	●								●	●					●		●		●						
NORMAL CONDITIONS — VITAL AREA	ESTABL. AUTH. ACTIVITIES & COND.																●	●													
	PROVIDE SURVEILL. PROC. & CNTLS.						●								●	●	●	●	●					●	●						
	FOR FACILITY PERSONNEL																														
	PROVIDE ESCORT PROC. & CONTROLS																			●											
	FOR AUTHORIZED VISITORS																														
	SENSE UNAUTH. ACTIVITIES & COND.	●	●	●	●	●	●														●		●		●						
	MAINTAIN EQUIPMENT IN										●																				
	OPERATING CONDITION																														
	PROVIDE AUXILIARY POWER							●	●	●																					


CONTROLS FOR ACTIVITIES/CONDITIONS
EQUIPMENT AND/OR DESIGN FEATURES
PROCEDURES
PERFORMANCE CHARACTERISTICS
TAMPER-INDICATING CIRCUITRY
CAPACITANCE ALARMS
MICROWAVE SYSTEMS, INTERIOR
INFRARED SYSTEMS, INTERIOR
ULTRASONIC AND SONIC SYSTEMS
CCTV SYSTEMS
EMERGENCY BATTERY SYSTEMS
EMERGENCY GENERATOR SYSTEMS
UNINTERRUPTIBLE POWER SYSTEMS
EQUIPMENT CHECKS/MAINTENANCE
CCTV MONITORING/SURVEILLANCE
DIRECT MONITORING/SURVEILLANCE
ESCORTS
GUARD PATROLS
EMERGENCY EVACUATION PROCEDURES
EMERGENCY ACCESS/EGRESS PROCEDURES
EMERGENCY CONDITIONS
PROTECTED AREA
MAT'L ACCESS AREA
VITAL AREA
PROV. EVAC. PROC. & CONTROLS
FOR FACILITY PERSONNEL
PROVIDE ESCORT PROC. & CONTROLS
FOR EMERGENCY PERSONNEL
SENSE UNAUTH. ACTIVITIES & COND.
PROV. EVAC. PROC. & CONTROLS
FOR FACILITY PERSONNEL
PROVIDE ESCORT PROC. & CONTROLS
FOR EMERGENCY PERSONNEL
SENSE UNAUTH. ACTIVITIES & COND.
PROV. EVAC. PROC. & CONTROLS
FOR FACILITY PERSONNEL
PROVIDE ESCORT PROC. & CONTROLS
FOR EMERGENCY PERSONNEL
SENSE UNAUTH. ACTIVITIES & COND
MAINTAIN EQUIPMENT IN
OPERATING CONDITION
PROVIDE AUXILIARY POWER

DISTRIBUTION:

U.S. Nuclear Regulatory Commission (50 copies for AN)
Division of Document Control
Distribution Services Branch
7920 Norfolk Avenue
Bethesda, MD 20014
Attn: P. Larkins

U.S. Nuclear Regulatory Commission
Division of Safeguards
MS SS881
7915 Eastern Avenue
Silver Spring, MD 20852
Attn: P. A. Dwyer (5)

Allied-General Nuclear Services
P.O. Box 847
Barnwell, SC 29812
Attn: P. E. Ebel (5)

400	C. Winter
1000	G. A. Fowler
1230	W. L. Stevens, Attn: R. E. Smith, 1233
1700	W. C. Myre
1710	V. E. Blake
1720	C. H. Mauney
1730	J. D. Kennedy
1750	J. E. Stiegler
1760	J. Jacobs
4400	A. W. Snyder
4410	D. J. McCloskey
4412	J. W. Hickman
4413	N. R. Ortiz
4414	G. B. Varnado
4416	L. D. Chapman (5)
4416	K. G. Adams
4416	J. A. Allensworth
4416	H. A. Bennett (7)
4416	D. Engi
4416	L. M. Grady
4416	C. P. Harlan
4416	R. D. Jones
4416	M. T. Olascoaga (7)
4416	C. J. Pavlakos
4416	D. W. Sasser
4416	D. R. Strip
8266	E. A. Aas
3141	T. L. Werner (5)
3151	W. L. Garner (3)
	For: DOE/TIC (unlimited Release)
3154-3	R. P. Campbell (25)
	For NRC Distribution to NTIS

☆U.S. Government Printing Office: 1980 — 677-116/531