NOT
MEASUREMENT
SENSITIVE

DOE G 470.4-1
Approved: 8-21-08

ASSET PROTECTION ANALYSIS GUIDE

[This Guide describes suggested nonmandatory approaches for meeting requirements. Guides are not requirements documents and are not to be construed as requirements in any audit or appraisal for compliance with the parent Policy, Order, Notice, or Manual.]

U.S. DEPARTMENT OF ENERGY
Office of Health, Safety and Security

AVAILABLE ONLINE AT:
www.directives.doe.gov

INITIATED BY:
Office of Health, Safety and Security

CONTENTS

ASSET PROTECTION ANALYSIS

1. INTRODUCTION. The U.S. Department of Energy (DOE) has for years conducted extensive and in-depth vulnerability assessments (VA). The VA process is an objective, systematic approach to evaluating protection effectiveness and for documenting the results of that evaluation. In the past, DOE security organizations have sometimes equated the application of the formal logic of the VA process with the complex and expensive computer tools used to evaluate the overall system effectiveness of a site's protection strategy for high-consequence assets (e.g., Category I special nuclear material [SNM] or radiological sabotage). Use of these tools requires large investments of time, money and other resources and yield results that can be justified only by the consequences of a failure to protect a high-consequence asset. The VA process within which these tools are used, however, can profitably be applied to a large class of evaluations that do not require a large investment of time and resources. The Asset Protection Analysis Guide is designed to aid sites in identifying these relatively low cost opportunities to enable managers to make informed decisions regarding protection options. While all applications of the VA process can correctly be called vulnerability analysis, this Guide will use the term "asset protection analysis" when discussing analysis using the approach outlined in this Guide.

   The Guide provides examples of the application of asset protection analysis to several common problems. Examples include an analysis of nonconforming storage for classified matter, a preliminary analysis of theft/sabotage targets that may not require a comprehensive VA, an analysis of security measures supporting temporary construction within a protected area (PA), security of a high-value theft asset that is not deemed a high-consequence target, and a roll-up analysis of Category III SNM. (Note that the results of any of these analyses may indicate the need for a more detailed VA.)

   Particularly, in situations where conditions or unseen factors render full compliance with established standards impractical, the Guide provides security professionals a relatively simple means of determining if the protection afforded a Departmental asset is acceptable and documenting this result.

   The process can be started by posing one or more of the following questions:

   - Is the protection system equivalent to Departmental requirements?
   - Is the adversary goal (sabotage, theft, roll-up, etc.) credible, and if not, why not?
   - Does the current protection system meet or exceed a particular standard, and is that acceptable?

   The security professional will need to have a good understanding of protection concepts such as target identification, detection, delay, and response.

2. OBJECTIVE. The objective of the VA process is to provide security and management staff with information to make informed decisions regarding the application of protection measures. Application of the asset protection analysis technique to common,

but less complex, issues that arise when implementing a graded protection philosophy can also provide important information to support management decision making. This process can also be used to quickly assess the impact of changes on the effectiveness of a protection system. While many of the examples could be performed by one person, experience has shown that a team rather than an individual approach can provide significantly better results by providing "sanity checks," an opportunity to critique ideas and approaches, and an additional data collection resource.

3. SCOPE.

a. Target Audience. The asset protection analysis process is designed for use by security professionals who generally are not involved in facility VAs; however, VA analysts may choose to add this information to their "analytical tool kit." Personnel should have adequate knowledge of the components of a comprehensive safeguards and security program.

b. Analysis Parameters. Examples in the Guide illustrate how the asset protection analysis process applies to a wide range of common problems for which the more detailed and laborious computer simulation methods may be inappropriate or inadequate. A quick, simple analysis is always preferred to no analysis, and in many cases is sufficient. While the process and philosophy presented in this Guide are similar to those required for the Department's most valuable assets, this process is not a substitute for approved methods nor should anything in this Guide be construed as relieving sites from the requirement to perform more complex assessments.

c. Classification. Risk Analyses maybe classified or unclassified sensitive and should be developed and protected until formally reviewed for a classification determination.

4. PROCESS.

a. Basic Asset Protection Analysis Process. Figure 1 is an overview of the asset protection analysis process when a comparative analysis is not required. The process is identical to the more extensive VA process published elsewhere, but is substantially simplified. Examples that support this figure are covered in Appendices B, C and D. The major components are further defined below:

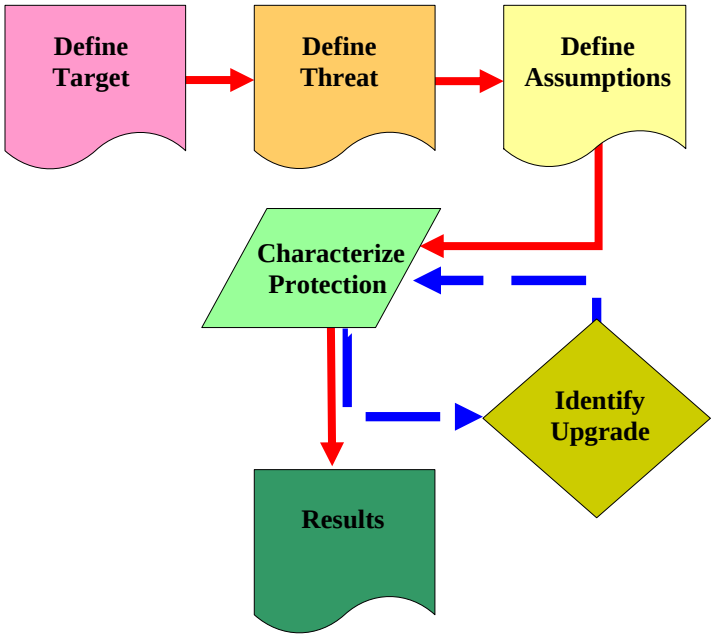


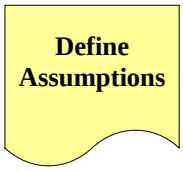
Figure 1. Asset Protection Analysis Flowchart

Target definition should include all the characteristics that will be significant in the analysis. For example, when analyzing theft of a target the size and transportability of the target, is a key consideration. However, when considering a sabotage-in-place event, size and transportability of the target may not be significant. Part of the target definition is the consequence associated with the loss or unauthorized exploitation of the target. This applies to theft, both abrupt and protracted, diversion, and sabotage. In addition, the security professional should consider other factors such as target conditions, facility operations, target configurations, and associated adversary task times. In most cases, the target should not be generalized, but rather each target should be analyzed separately.

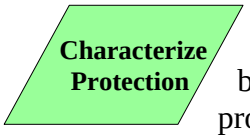
The threat definition should be consistent with the threat discussed in the Design Basis Threat[1] augmented by any additional threats that may be local in nature. Part of the threat definition should include the end goal of the adversary. For example, with classified matter the goal of the adversary may be the theft of an item or simply obtaining classified information by exploiting the item in place (e.g., photographing it, measuring its' dimensions). Other adversary goals could include the theft or sabotage of biological targets, interruption of crucial operations like a badge

[1] The performance metric for security design has been provided since 1983. the DBT or it's successors should be used for the analysis.

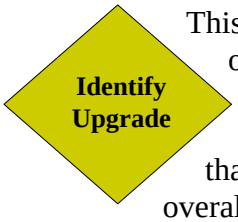
office or alarm station or the theft of a high-value asset (e.g., precious metals, supercomputers). Additional guidance may include local and/or regional threat guidance. This guidance should be used to refine the applicable threat and should not be used to reduce or diminish it. In addition, all applicable DOE/National Nuclear Security Administration (NNSA) memoranda should be reviewed for additional threat clarifications and guidance.



All assumptions used in this process need to be defined. This step may need to be revisited following the target and threat definition steps. These assumptions should include what adversary action(s) is considered successful. Adversary success criteria might include the theft of a classified part or interruption of a critical mission. Any assumptions that are key to the result should be identified. For example, in a particular case one may assume that two delays are similar (in the absence of specific data), that a posted Security Police Officer (SPO) provides a similar detection probability to that provided by volumetric detection, or that an unarmed response will be sufficient to interrupt (halt) adversary actions. Assumptions should be documented and include the rationale for each assumption.



This should include all security systems that contribute to the overall protection of the target, including security layers and boundaries, applicable detection, delay, access controls, and protective force response, armed or unarmed, or local law enforcement. Non-security measures that can add to the overall protection effectiveness, such as plan of the day procedures, limitations on access due to required safety training, etc. should also be included. The protection characterization may also show loss detection as part of the overall protection of the asset. The description need not be the detailed characterization used in traditional VAs but a brief portrayal of all protection elements. This characterization need not discuss specific numeric values (e.g., probability of detection [P_D], travel times, delay, task times, and response times) unless they contribute to the overall protection analysis of the target. The characterization should be detailed enough so that the security professional can perform the needed comparison (next step). The security professional may choose to use a table presentation to organize the information (see Appendices).



This step should be performed only if the comparison shows a lack of adequate protection. However, if reasonable enhancements are identified as a result of the analysis, they may be listed here. Whenever possible, upgrades should be recommended that can be implemented in a timely manner and will benefit the overall protection of the target. The system upgrades discussed should explicitly show protection improvement. Consideration should be given to the compatibility of proposed changes with the overall facility design requirements.

This step summarizes the results and conclusions reached as a result of the analysis. A table depicting the results of each case evaluated or, in the case of a comparative analysis, the comparison of the compliant with the nonconforming for each case analyzed should be considered to summarize results. Identification of critical protection elements, if any can be discerned, should be included to indicate that these elements may need additional focus to ensure that they function as expected. This section might also discuss possible upgrades. If the results from this analysis are unclear, the results section should identify that fact and indicate whether further analysis, perhaps using the more complex VA/system effectiveness determination, should be performed.

b. Comparative Analysis. Figure 2 is an example of the comparative analysis process. This process is the asset protection analysis process depicted above with the addition of steps to allow comparison of the existing protection with some protection standard, such as a General Services Administration (GSA)-approved container, a vault-type room (VTR), or some industrial standard that may be chosen as a standard for some asset. The examples depicted in Appendices A and E reflect the application of comparative analysis to two typical problems. The two additional elements incorporated into the comparative analysis process are outlined below:

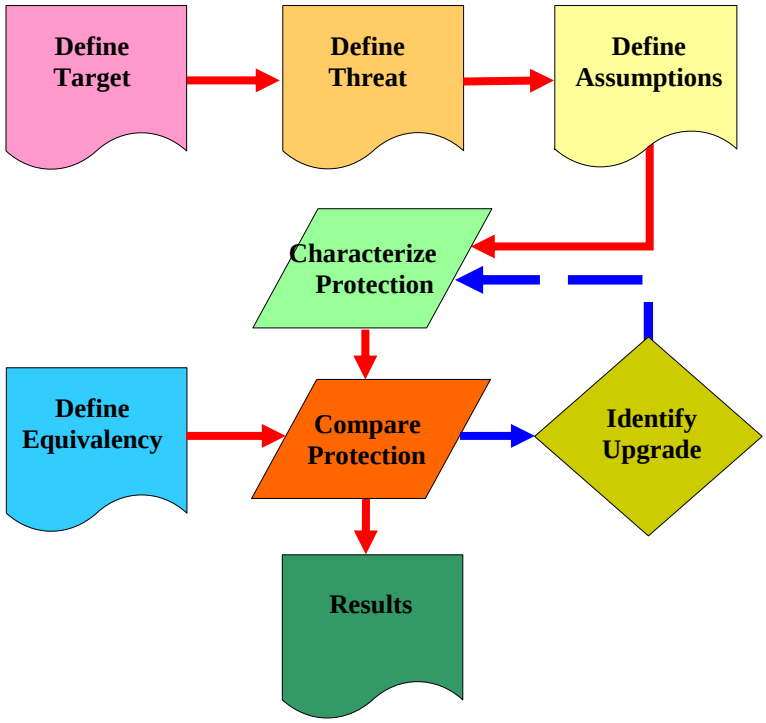
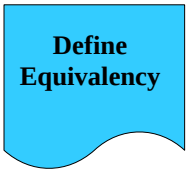
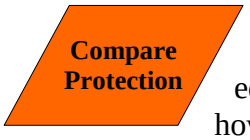


Figure 2. Comparative Analysis Process



A comparative analysis is normally undertaken when some characteristic of the target prevents the application of a standard protection design. For example, there are classified items that will not fit into GSA-approved containers or there are processes involving classified information or matter that cannot be contained in a VTR. In order to define equivalency, the security professional identifies a protection standard that might be applied to an asset of similar concern (e.g., a VTR for open storage of Secret classified matter) and defines the essential protection measures provided by that protection standard. The definition should focus on the portions of the standard that provide compliance with applicable requirements for a VTR (e.g., interior alarm coverage, access controls). The requirements used for this step should reflect Departmental requirements and should not include any local enhancements to requirements or special features of a particular application at the site (such as locating a VTR within a PA). The level of detail should be similar to that performed in the previous step.



In this step, the analyst compares the protection of the target in question with a compliant standard protection for an equivalent case. The security professional will need to define how this comparison is performed. The comparison may be a layer by layer or element by element comparison. The focus of this step is to compare the protection effectiveness along the complete adversary pathway that leads to adversary success. This comparison should describe, but not compare specific adversary actions since the comparison should be at the level of the complete adversary pathway/task. The results of the comparison will contrast the protection that would be afforded the target in question if it were possible to place it in a standard protection configuration with that provided in the actual configuration. The goal is to determine and document that the target is protected at least as well as it would be if it were in a standard protection posture. If not, the analyst should determine what additional protection elements should be added to achieve equivalent protection. Often these comparative results are best presented in a table.

5. SUPPORTING DOCUMENTATION. The analyst should be prepared to defend any assumptions and/or element performance parameters that support the asset protection analysis. To this end, documentation used or created as a result of the analysis should be maintained and filed for future use and for review in validation efforts. Examples of documentation to be maintained may include, but are not limited to:

- Basis for any assumptions
- Applicable policy requirements
- Description of protective systems
- Performance testing data if used
- Data used but not explained in the process.

6. EXAMPLES. Asset protection analysis is useful for addressing many common issues. The following examples illustrate the application of the process to five specific situations. The examples provided in Appendices A through E of this Guide should not be interpreted as the only applications for this methodology. The examples are merely provided to illustrate how this process can be applied to a variety of situations. None of the examples should be interpreted as clarification of Departmental policy. The examples provided are entirely fictional, and the values used for assessment, detection, and delay are not supported by real data or testing. So that the Guide may remain unclassified, the threat used in the examples does not correlate with the Design Basis Threat (or subsequent replacement or relevant document). However, when performing an asset protection analysis for actual targets, the current DOE threat guidance along with any other programmatic guidance that may apply should be used to define the threat pertaining to a particular target.

APPENDIX A: NONCONFORMING STORAGE OF CLASSIFIED MATTER

1. REQUIREMENTS. Numerous requirements are prescribed in DOE M 470.4-2, *Physical Protection*, and DOE M 470.4-4, *Information Security*.

2. SITUATION. The facility stores classified radioactive waste (including Secret Restricted Data [SRD] weapons parts) within a protected area (PA) but outside a material access area (MAA) while awaiting final disposition for the waste. The material is stored in large, sealed (tamper indicating) canisters providing containment for the radioactive waste as well as some radiation shielding. The required canisters are too large to fit within any available General Services Administration (GSA)-approved container; therefore, the SRD would require storage in a vault-type room (VTR), or vault, within a limited area (LA) for fully compliant storage. Due to the nature of the material in the canisters and local operating conditions, an area meeting the requirements for a VTR is not available, and yet it is an operational necessity that the waste and weapons parts be placed in canisters and stored for an indefinite time while awaiting disposition.

Any one of the SRD weapons parts comingled with other radioactive waste in the sealed containers would be considered a target. Individual weapons parts are person-portable and could be placed in a GSA-approved container, but the sealed containers required for safe handling are too large to fit in a GSA-approved container and are not person-portable.

(This threat definition is used for illustration. It does not necessarily reflect a threat derived from the Design Basis Threat (or subsequent replacement or relevant document)) The Design Basis Threat (or subsequent replacement or relevant document) defines the following adversary characteristics:

- One or two individuals with technical backgrounds who will carry out the theft assisted by one individual who is familiar with operational and general security provisions in and around the target material.

- Neither those engaged in the actual theft nor the individual providing information is willing to employ violence to achieve success.

Note: So that the Guide may remain unclassified, the threat used in the examples may not correlate with the Design Basis Threat (or subsequent replacement or relevant document). However, when performing an actual analysis the current DOE threat guidance should be used.

Define Assumptions

- The adversary desires to physically remove the target for detailed study and exploitation.
- LAs and VTRs meet all requirements.
- PA meets all security requirements.
- Safety controls on radioactive waste canisters are rigorously applied by all except thieves.

3. SCENARIOS. As described, the threat group might or might not have access to plant property or security areas within the plant. Since the required actions are very different for these cases, the overall problem is broken into cases:

   a. Case 1. The thief or thieves have unchallenged access to the property protection area (PPA) only.

   b. Case 2. The thief or thieves have unchallenged access to LAs within the PPA, but not the PA. In the case of the VTR comparison, this would equate to access to LAs within the PPA but not the VTR itself.

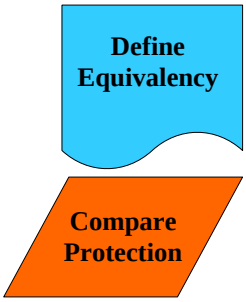
   c. Case 3. The thief or thieves have unchallenged access to the PPA, LA, and the PA. In the case of the VTR comparison, this would equate to access to LAs within the PPA and the VTR itself.

   In the case of the VTR comparison, no equipment would be necessary. When attempting to acquire the SRD material from the radioactive waste canister, either the thief or thieves should have tools to open the canister or have a means of transporting the container.

   In the case of the VTR, the thief or thieves should pick up the item and place it out of sight without being observed by persons in the area. In the case of extracting the target from the waste container, a container holding SRD material should be correctly identified, the container should be opened and the part found, extracted, and hidden without observation and without leaving sufficient evidence to create an alarm before they leave the area. In the case of extracting the container itself, the thief or thieves should correctly identify a container holding SRD material, place it on whatever device is being used to transport it, and exit the PA and PPA with the canister.

Characterize Protection

While the individual weapons parts could be stored in a GSA-approved container, the problem is to provide protection while in the radioactive waste canister awaiting shipment. Since that assembly would require storage in a VTR, a VTR will be the standard storage configuration used for comparison.



In this example, DOE requirements specifically define protection standards.

The three cases involving the comparison of the VTR and nonconforming storage are analyzed below.

d. Analysis of Case 1.

(1) VTR. Thieves advance through the PPA to the entrance to the LA boundary. They cannot bypass access controls at the authorized portal. They wait for late night and successfully force entry at another point on the LA boundary. They then proceed to an exposed surface of the VTR and force entry. Upon entry into the VTR, they are detected, an alarm response is initiated, and they are unable to obtain the target and escape the protective force response.

(2) Nonconforming. Thieves advance through the PPA to the entrance to the PA boundary. They cannot bypass access controls at authorized entry portals. They wait for late night and attempt to force entry through the Perimeter Intrusion Detection and Assessment System (PIDAS). They are detected, an immediate armed response occurs, and they are apprehended shortly after penetrating the inner PIDAS fence.

e. Analysis of Case 2.

(1) VTR. Thieves choose a time when the VTR and the immediate area of the VTR is typically unoccupied. They advance through the PPA to the entrance to the LA boundary and on through the LA boundary without detection. They are unable to manipulate the VTR lock so they force entry through a wall surface. Upon entry into the VTR, they are detected, an alarm response is initiated, and they are unable to obtain the target and escape the protective force response.

(2) Nonconforming. Thieves advance through the PPA to the entrance to the PA boundary. They cannot bypass access controls at authorized entry portals. They wait for late night and attempt to force entry through the PIDAS. They are detected, an immediate armed response occurs, and they are apprehended shortly after penetrating the inner PIDAS fence.

f. Analysis of Case 3.

(1) VTR. Choosing a time when the VTR is otherwise unoccupied, the thieves traverse the PPA and LA portals using their approved access, open the VTR door, and place alarms in access mode. They proceed to locate the

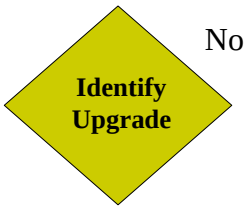
SRD item and place it in a container brought with them to conceal the object's shape. They then close the VTR, following all procedures, and exit the site. The loss of the item is noted shortly after the VTR is opened in the morning. The record of access by the thieves is clear, and attempts to apprehend them begin immediately.

(2) Nonconforming. Thieves realize that they will probably be unable to open or move a canister without action being taken to stop them. They initially attempt to acquire the authorization to access and/or remove the canister. They are prevented from obtaining such authorization by the safety and operational controls governing such actions, even though they are able to avoid raising suspicion in the attempt. Choosing a time when routine work with hand tools would not be unusual within the PA, they use their authorized PA access to enter the PA with the minimum hand tools required to open a canister.

(a) Alternate scenario 1. They proceed to a canister containing SRD, open it, and begin to look for a classified weapons part. Their actions are observed by other workers, deemed a clear violation of radiation safety requirements, and their effort is halted.

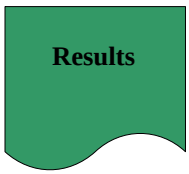
(b) Alternate scenario 2. They are able to find an SRD part and depart the area. They are discovered to be attempting to remove an unusual item at the PA exit portal, and subsequent investigation results in identification of a radioactive material spill in the vicinity of the canisters, contamination of their hand tools, and identification of the weapons part, resulting in their apprehension.

4. UPGRADE OPTIONS.



No upgrades were identified as necessary for providing adequate protection under the prescribed nonconforming storage configuration.

5. SUMMARY AND CONCLUSIONS.



As can be seen from the table below, the nonconforming storage method outperformed the minimally compliant standard method when all elements of both are performing as designed. Therefore, the noncompliant storage option provides equivalent protection needs for the material.

Table A-1. Summary of Results

Case	VTR	Nonconforming
Case 1	Compliant (stopped during escape)	Equivalent or better (stopped before acquiring target)
Case 2	Compliant (stopped during escape)	Equivalent or better (stopped before acquiring target)
Case 3	Compliant (timely detection of loss)	Equivalent or better (stopped before acquiring target or during escape)
Overall Rating	Compliant	Equivalent or better

Critical elements of the nonconforming storage configuration that should be tested periodically (in addition to the required testing for the PIDAS, portals, etc.) are:

- The difficulty of obtaining permits to open radioactive waste containers,
- The reaction of the plant population to opening radioactive waste containers, and
- The ability of portal Security Police Officers to recognize items that are potentially classified.

APPENDIX B: SECURITY FOR A VISITOR CONTROL OFFICE

1. REQUIREMENTS. DOE M 470.4-2, Chapter XV, *Physical Protection*, "Stocks of badging materials, unissued DOE security badges, and badge-making and processing equipment must be stored to protect against loss, theft, or unauthorized use." No other requirements specifically address the protection of a visitor control or badge office.

2. SITUATION. The visitor control facility resides in an area designated as a property protection area (PPA). The visitor control office is the only visitor control facility onsite and is also where site badges are manufactured. The primary requirements associated with badge/visitor control facilities are the protection of badging materials and equipment.

The target is a commercially available badging system. All badging stock is stored in a General Services Administration (GSA)-approved container. Badge production equipment and other badging supplies are in a windowless, locked room inside the PPA boundary. (Replacement equipment for manufacturing badges is available from the manufacturer in less than one week.) Access to the PPA during regular business hours is by posted Security Police Officer (SPO). Access to the PPA during off-hours is by badge reader through a card reader-controlled door. Access to the visitor control office is controlled by a cipher lock, and the cipher code is given only to visitor control personnel. The perimeter of the PPA is randomly patrolled by an unarmed SPO, but at least once every four hours. No interior PPA patrol is used. There is no intrusion detection provided at the visitor control office.

(This threat definition is used for illustration. It does not necessarily reflect a threat derived from the Design Basis Threat (or subsequent replacement or relevant document).) The Design Basis Threat (or subsequent replacement or relevant document) defines the following adversary characteristics:

- Outsiders: Two individuals with good technical backgrounds who are unwilling to use violence and are assisted by a single insider who only supplies information regarding the target location, visible security systems, and operational schedules.
- Insider: The insider was considered in the assessment.
- Possible theft of badging stock.
- Possible sabotage of badging equipment.
- Manufacture of a badge that will permit access to other site security areas.

Note: So that the Guide may remain unclassified, the threat used in the examples may not correlate with the Design Basis Threat (or subsequent replacement or relevant

document). However, when performing an actual analysis the current DOE threat guidance should be used.

Define Assumptions

- The goal of the adversary is to gain access to the visitor control office and make a badge that will grant entry into the Site's Limited Areas (LA) for the purpose of stealing classified information.
- The adversary will cease activities if interrupted by one or more responding SPOs or local law enforcement.
- The adversary will attempt the activity during off-hours.
- Site security systems are operational and work according to prescribed requirements. This assumption is based on the most current inspections, maintenance records, self assessments, training, etc.

Characterize Protection

See Table B-1, Protection System Characterization – Visitor Control Office.

Table B-1. Protection System Characterization – Visitor Control Office

Protection Element	Function	Effective Against	Compliant with Requirements	Comments
Building Perimeter				
- Masonry Construction	Delay	Outsider	Yes[1]	PPA Perimeter
- Locked Personnel Doors	Delay and Access Control - 10 seconds[2]	Outsider	Yes	PPA Perimeter
- Windows	Delay	Neither	Yes	PPA Perimeter
- Ventilator Ducts covered with steel grating	Delay	Outsider	Yes	PPA Perimeter
Visitor Control Office				
- Walls – Sheetrock over studs (floor to true ceiling)	Delay – 15 seconds w/hand tools[3]	Outsider	NA[4]	
- Locked Personnel Door	Delay and Access Control - 10 seconds[5]	Outsider	NA	
Access Controls				
- Automated Access Control System on PPA doors	Access Control	Outsider	Yes	PPA Perimeter
- GSA-Approved Container	Physical and Access Control	Outsider	Exceeds Requirements	

[1] Compliant with PPA requirements. No specific design requirements exist for the protection of a badge office.
[2] Sandia Barrier Handbook *(fictional)*
[3] Ibid
[4] Not Applicable. No specific construction requirements exist for the protection of a badge office.
[5] Sandia Barrier Handbook *(fictional)*

Protection Element	Function	Effective Against	Compliant with Requirements	Comments
- Passwords for computer systems	Access Control	Outsider	Yes	
- Cipher locked Visitor Control Office Door	Access Control	Outsider	NA	
Intrusion Detection System				
- Four hour exterior patrol	Detection	Outsider	Yes	PPA Perimeter

3. SCENARIOS.

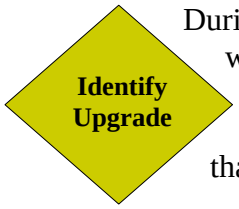
a. Analysis of Case 1. An outsider adversary would need to gain access to the PPA. If the adversary attempted to violate the door, it would generate a forced entry alarm and cause a response. If the adversary attempted to gain entry into the PPA through a window, signs of a forced entry would be detected but detection may not be timely. Since there is a low probability of timely detection, this would be the preferred entry for the adversary. Once inside the facility, the adversary would need to gain access to the badging office. The mechanical cipher lock on the door will provide only minimal delay and could be manipulated without leaving signs of entry. For the purpose of this example, the adversary was able to manipulate the cipher lock. Once inside the badging office, the adversary has access to the equipment but now should gain access to the badge stock in the GSA-approved container. Forced entry into the container provides delay, but the delay is measured in minutes, so it is well within the SPO patrol times. However, forced entry will again prevent surreptitious entry into the container but will have low probability of timely detection. Successful to this point, the adversary should now attack the computer system to gain access to the mainframe housing the program necessary to make the badge. Without the password, the adversary cannot access the system. Since the application resides on the mainframe, stealing the computer, badge stock and other equipment for manufacturing the badge will provide the adversary little benefit. However, if the adversary does successfully steal the equipment and stock, the evidence of the crime will be obvious and local procedures will prevent the stock from being used to gain access.

b. Analysis of Case 2. An insider who is not a part of the visitor control office or badging operations, with limited access, can go unchallenged up to the visitor control office door. Once the insider has reached the door, the insider is faced with the same challenges and choices faced by the outsider. An additional challenge for this particular insider is that by using their authorized access up to the visitor control office door, there is now a record of their identity and the time and date the facility was accessed. The resulting investigation would make this insider a prime candidate for the activity. This fact would likely weigh heavily on the decision process for this scenario.

c. Analysis of Case 3. An insider who works in the badge office would be successful in making a counterfeit badge that would meet the objective of the scenario. This scenario would most likely be successful for either duty hours or off-duty hours.

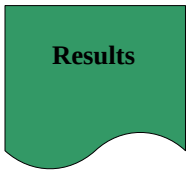
However, the challenges faced by this insider would be significant. For example, there would be audit trails leading directly back to them. This adversary would have left an audit trail of their identity and the date and time they accessed the PPA, logged onto the computer system, and accessed the badging program.

4. UPGRADE OPTIONS.



During the conduct of this assessment, it was determined that upgrades were not needed. However, administrative procedures such as audit trails, badge stock inventory, and strict control of access to the GSA-approved container housing the stock are additional measures that might enhance the protection of the badge office.

5. SUMMARY AND CONCLUSIONS.



Departmental directives do not explicitly identify protection measures for the badging stock, equipment or process beyond protection from theft or unauthorized use. The example shows that the assets require more than mere PPA physical security requirements in order to be compliant. The security professional should be able to determine and defend the analysis. In the example, there were measures in place that exceeded basic PPA physical security requirements. Those extra security measures, mainly the access control system for entry into the PPA and the GSA-approved container, preclude all but the badge office employee from surreptitiously making a counterfeit DOE badge or theft of badge stock and equipment. In this particular case, the analyst should also review site procedures related to events if site badge stock was missing. This would also be an excellent indicator to determine if current security measures and practices meet the intent of the requirement.

- Cases 1 and 2 would be extremely difficult to accomplish without signs of forced entry. The other consideration is that if the adversary was successful, the actions would grant access only to the LA and would not allow access to classified information due to the Department's security in-depth strategy.

- Case 3 is, in all cases, the most difficult because the insider has all necessary authorizations. However, administrative procedures such as audit trails, badge stock inventory, and strict control of access to the GSA-approved container housing the stock are additional measures that could thwart this type of attack.

Table B-2. Summary of Results

Case	Visitor Control Office
Case 1	Equivalent or better
Case 2	Equivalent or better
Case 3	Equivalent or better
Overall Rating	Equivalent or better (replacement of sabotaged equipment)

APPENDIX C: ANALYSIS TO DETERMINE THE CREDIBILITY OF ROLL-UP

Roll-up is the accumulation of smaller quantities of special nuclear material (SNM) to a higher category based upon U.S. Department of Energy (DOE) M 470.4-6 Chg 1, *Nuclear Material Control and Accountability*, dated 8/26/2005. Unless it has been demonstrated by a vulnerability assessment (VA) that roll-up is not credible, SNM must be safeguarded and protected based on the total quantity of SNM for a location (e.g., material access area, protected area, building, or group of buildings) (DOE M 470.4-6 Chg 1, Section A, Chapter 1, paragraph 2.c).

In this example analysis, it is assumed that several locations within a single building contain Category III or lower quantities of SNM. It has been demonstrated previously that roll-up of material within the subject building in combination with other materials onsite is not credible. Each location within the building is protected in accordance with safeguards and security policy for protection of Category III materials. The problem is to determine whether there is a credible roll-up scenario that would require the application of Category II protection standards to the building given that all the material assembled in one location would be a Category II quantity. Below is a report that might be generated as a result of applying the asset protection analysis principles described in this Guide to this problem.

1. REQUIREMENTS. Category III quantities of SNM must be stored within a locked security container or room, either of which must be located within at least a Limited Area (LA). The container or room must be under the protection of an intrusion detection system (IDS) or protective force (PF) patrol physical check at least every 8 hours (DOE M 470.4-2 Chg 1, Section A, Chapter 2).

   Category II quantities of SNM are protected by a much more robust set of protection measures that are not described here because the question is whether roll-up to Category II is credible, not what protection is to be applied if it is.

2. SITUATION.

The seven MBAs contain various quantities of SNM in a range of forms. In all cases, the SNM is person-portable and constitutes a Category III quantity. The MBAs are located within a single large multi-floor building on three floors. The MBAs holdings are identified below:

- MBA I: Category III Attractiveness Level B plutonium metal
- MBA II: Category III Attractiveness Level B plutonium metal
- MBA III: Category III Attractiveness Level C plutonium oxide
- MBA IV: Category III Attractiveness Level C plutonium oxide
- MBA V: Category III Attractiveness Level C plutonium oxide
- MBA VI: Category III Attractiveness Level C plutonium oxide

- MBA VII: Category III Attractiveness Level C plutonium oxide

Define Threat

Since Departmental policy does not specify adversary numbers and characteristics for a roll-up attempt, the following threat is defined only for purposes of this analysis. The threat described here is used for purposes of illustration and does not constitute an approved threat for rollup scenarios. The appropriate threat should be determined through appropriate consultation and coordination with DOE/NNSA officials.

- Outsiders: The outsider has good organizational and tactical skills. The outsider, by definition, does not have authorized access to the facility. The outsider has the tools necessary to accomplish the mission but is neither equipped nor willing to resist the PF if directly challenged. The outsider is assisted by one insider who provides detailed information regarding the SNM location and the security system design.

- Insider: One active, nonviolent insider with knowledge of the target. The insider is not willing to risk detection.

The site is an open campus design. The Central Alarm Station (CAS) is staffed by an unarmed Security Police Officer (SPO) 24 hours a day, 7 days a week. The CAS controls radio communications and has a direct link to local law enforcement, which has signed a mutual assistance agreement with the site.

Note: So that the Guide may remain unclassified, the threat used in the examples may not correlate with the Design Basis Threat (or subsequent replacement or relevant document). However, when performing an actual analysis the current DOE threat guidance should be used.

Define Assumptions

Building 1126 contains seven Category III Material Balance Areas (MBAs) located within a single LA. Based on an analysis by the nuclear material control and accountability group, the combined holdings of the seven MBAs constitute a Category II quantity of SNM. This VA has been conducted to determine whether there are credible roll-up scenarios where a Category II quantity of SNM may be accumulated.

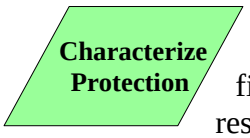
- Only SNM located in the LA is to be considered.

- The MBAs comply with DOE requirements.

- The adversary goal is to obtain a Category II quantity of SNM and its removal from the site.

- The response of the PF to an LA alarm is 20 minutes, including alarm assessment and dispatch.

- Once interrupted by the PF, the adversary will attempt to escape but will not offer physical resistance to the PF.



The day shift patrol complement is four armed SPOs. Two are assigned foot patrol duties in the main administrative area, serve as first responders to the administrative areas of the campus, and would not respond to Building 1126 located across campus. The other two SPOs operate single-person patrol vehicles, patrol other buildings of the site, and would serve as first responders to Building 1126. On the off-shift, two armed SPOs are assigned to single-person vehicle patrols. In all cases, the vehicle patrols can respond to Building 1126 in 20 minutes or less.

Building 1126 constitutes the LA. The exterior walls of the LA are constructed with filled 8-inch concrete masonry units. The interior walls extend from the floor to the true ceiling. They are constructed of sheetrock attached to metal studs. Five standard fire doors provide emergency egress from the LA. All emergency exit doors are equipped with balanced magnetic switch (BMS) alarms secured at all times. Normal ingress into the building is controlled by an automated access control system. The LA has no exterior windows on the ground level, and exterior ventilation ducts are equipped with ¾-inch steel bars horizontally and vertically on 6-inch centers.

Access to Building 1126 is controlled during operational hours by a turnstile. Unescorted building access requires a badge swipe and personal identification number (PIN) entry. A receptionist ensures escorts are assigned to uncleared visitors. Cleared visitors are entered into the site access control database for tracking purposes and have unrestricted access to the area but only for the duration of the visit. The access control database is located in the CAS. The main entry door is a standard plate glass door.

Each MBA nuclear material (NM) custodian and a material handler conduct daily administrative checks of the security container(s) located within the MBAs at the end of each business day to ensure material is appropriately secured. A materials surveillance program has been implemented that requires two authorized personnel to access any MBA.

a. MBA I, Room 326. Two doors provide access to the room, and both doors are equipped with BMS alarms controlled by an automated access control system. The target material is stored in a locked file cabinet. The time needed to gather the material once inside the room is approximately 10 minutes.

b. MBA II, Room 354. Two standard fire doors provide access to the room. Both doors are equipped with BMS alarms controlled by an automated access control system. The target material is stored in a locked file cabinet. The time needed to gather the material once inside the room is approximately 5 minutes.

c. MBA III, Room 301. The room is dedicated entirely to the storage of Category III quantities of SNM. Material within the room is not placed into a security container. The room is locked during nonoperational hours and is subject to random patrol checks at least once every 8 hours. The time needed to gather the material once inside the room is approximately 12 minutes.

d. MBA IV, Room 223. The room is locked and alarmed during nonoperational hours. The target material is stored in four locked glove boxes. The time to gather the material once inside the room is approximately 8 minutes.

e. MBA V, Room 287. The room is locked during nonoperational hours and is subject to random patrol checks at least once every 8 hours. The target material is stored in two General Services Administration (GSA)-approved security containers; each is equipped with an XO-9 combination lock. The time to gather the material once inside the room is approximately 20 minutes.

f. MBA VI, Room 134. The room is locked during nonoperational hours and is subject to random patrol checks at least once every 8 hours. The target material is stored in two glove boxes located in the room. The time to gather the material once inside the room is approximately 15 minutes.

g. MBA VII, Room 101. The room is dedicated entirely to the storage of Category III quantities of SNM. The room is locked during nonoperational hours and is subject to random patrol checks at least once every 8 hours. The target material is stored in a GSA-approved security container equipped with an XO-9 combination lock. The time to gather the material once inside the room is approximately 20 minutes.

3. SCENARIOS.

a. Outsider Scenario. The adversary enters the site during normal business hours equipped with common maintenance tools including electric drills and reciprocating saws. The adversary waits for darkness to begin the task. The adversary breaches a Building 1126 emergency exit door and gains access to the building. The adversary moves to MBA I, breaches the door, forces open the material storage location, and obtains the target material. The adversary then moves to MBA II and repeats the process. The adversary emerges from the target building in approximately 15 minutes and attempts to exit the site. This scenario is depicted in Tables C-1 and C-2.

Table C-1. Outsider Scenario MBAs I and II

Action	Detection Potential	Comments
Enter Site	Very Low	
Enter Building 1126	Moderate	Forced entry will cause an alarm and send a response
Move to MBA I and breach MBA	Moderate	Forced entry will cause an alarm and continue the response
Obtain MBA I material	Very Low	
Move to MBA II and breach MBA	Moderate	Forced entry will cause an alarm and continue the response
Obtain MBA II material	Very Low	
Exit Building	Very Low	

Action	Detection Potential	Comments
Exit Site	Very Low	
Overall Rating	**Ineffective Performance**	Two independent, moderate detection potentials upon building entry and entry into MBA I allow an assumption that the response would begin no later than entry into MBA I. Examination of the timelines above indicates that 18 minutes remain on the adversary timeline, indicating that, in the worst case response, interruption is unlikely to occur.

Table C-2. Outsider Scenario – MBAs I and IV

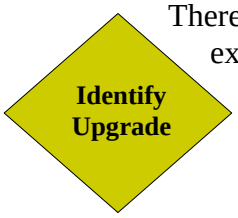
Action	Detection Potential	Comments
Enter Site	Very Low	
Enter Building 1126	Moderate	Forced entry will cause an alarm and send a response
Move to MBA I and breach MBA	Moderate	Forced entry will cause an alarm and continue the response
Obtain MBA I material	Very Low	
Move to MBA IV and breach MBA	Moderate	Forced entry will cause an alarm and continue the response
Obtain MBA IV material	Very Low	
Exit Building	Very Low	
Exit Site	Very Low	
Overall Rating	**Effective Performance**	Two independent, moderate detection potentials upon building entry and entry into MBA I allow an assumption that the response would begin no later than entry into MBA I. Examination of the timelines above indicates that 21 minutes remain on the adversary timeline, indicating that, in the worst case response, interruption is likely to occur.

Examination of the results show that the timelines associated with combining MBA II with either MBA III or IV provides similar results. That is, the system will likely be effective in outsider scenarios involving combinations of MBAs I and IV and MBAs II and III. However, the system is likely to be ineffective in outsider scenarios involving combinations of MBAs I and II and MBAs II and IV.

b. Collusion Scenario. During normal working hours, the adversary colludes with an insider who has access into Building 1126. Administrative controls requiring two-person access preclude single-person entries. At this point, the scenarios revert to the outsider scenario above since the adversary would resort to force to complete the mission. However, the assistance of the insider eliminates the moderate detection potential upon entering Building 1126. On the other hand, personnel in the building should hear the sound of breaking into an MBA or an

alarm should function with high probability if entry is through the alarmed door. Therefore, while the moderate detection potential at the building entrance is lost, a new moderate detection potential is created before the adversary accesses the material as the adversary attempts to force a door lock or create an entrance in a wall surface. Therefore, the use of a colluding insider changes the timeline for the outsider acting primarily by retarding a likely detection to the time of entry into the first targeted MBA. For calculation purposes, it will be assumed that the detection potential associated with employees noticing and investigating the disturbance associated with accessing the first MBA could occur at any time during that activity; therefore, the task time to enter the MBA is also eliminated from the adversary timelines. This results in timelines identical to the scenario where the outsider was acting alone. As was the case with the outsider scenarios, the system is likely to be ineffective in collusion scenarios involving combinations of MBAs I and II, and MBAs II and IV.

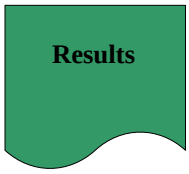
4. UPGRADE OPTIONS.



There are numerous upgrade options available to the site. Below is an example of three options:

- Option 1 – Limit the amount of SNM stored in the MBAs to ensure that roll-up is not possible. This option may not be viable because the site may need all the SNM stored in each MBA.
- Option 2 – Increase task times at the target areas, especially targeting MBAs II and IV.
- Option 3 – Decrease response time by modifying PF posts and patrols.

5. SUMMARY AND CONCLUSIONS.



The protection measures presently applied to the SNM assets in Building 1126 are not adequate to provide a high level of system performance. Therefore, it is recommended that one of the upgrade options identified be implemented.

APPENDIX D: HIGH-VALUE ASSET

1. REQUIREMENTS. The U.S. Department of Energy (DOE) has no set criteria for the protection of high-value assets unless they present a specific hazard to the public, environment, employees or impacts national security. The protection scheme, at a minimum, should be capable of detecting abrupt or protracted theft.

2. SITUATION. The site has an operational requirement for large quantities of platinum valued at more than $5 million. This material is stored in a property protection area (PPA). Management wants to know if the security system is adequate.

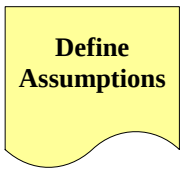
The platinum is in the form of small, cup-sized crucibles each worth approximately $1,500. The platinum does not activate standard metal detectors. The normal in-storage inventory is approximately 3,000 troy ounces or 225 pounds.

(*This threat definition is used for illustration. It does not necessarily reflect a threat derived from the Design Basis Threat (or subsequent replacement or relevant document).*) A review of recent incidents of major theft concludes the most likely outsider threat is a criminal, assisted by a single insider who provides operational and security system information.

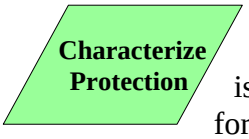
- Outsider: The outsider is likely to be armed with small-caliber automatic weapons and handguns. He/she has the capacity to develop and implement complex plans. He/she is not adverse to using violence.

- Insider: A single non-violent insider is the most likely insider threat. The insider may use two strategies, abrupt theft of a large quantity of platinum or protracted theft of small amounts. In either case, the insider wants to avoid detection.

Note: So that the Guide may remain unclassified, the threat used in the examples may not correlate with the Design Basis Threat (or subsequent replacement or relevant document). However, when performing an actual analysis the current DOE threat guidance should be used.



The outsider's goal is to obtain the whole inventory. The insider may choose an abrupt or protracted theft.



The platinum is used in a small manufacturing operation. The plant operates on a normal, Monday-Friday, single-shift schedule. Platinum is moved from the storeroom in response to production needs. The shift foreman and the furnace operator request specific numbers of crucibles to meet production needs.

The storeroom custodian removes the number of needed crucibles from the storeroom and provides a receipt to the furnace operator. At the end of the day, the furnace operator returns any unused crucibles to the storeroom custodian and is given a receipt. The foreman conducts a visual check of the furnace area at the end of the shift to verify no crucibles are left in the area. Storeroom records are audited monthly, and a physical inventory is conducted quarterly by the site's accounting office.

The plant is divided into three general areas: administration, manufacturing, and shipping/receiving. Access to the manufacturing portion of the plant (see Figure D-1) is controlled by an unarmed guard who visually checks badges and monitors a standard airport-style, walk-through metal detector. Employees and visitors are subject to random cursory inspections of hand- carried items upon exiting.

The manufacturing area is constructed of tilt-up concrete panels approximately 6-inches thick. There are no windows. The roof is made of 8-inch-thick interlocked concrete beams. The heating/ventilation equipment is mounted on the roof, and all roof penetrations are equipped with ¾-inch rebar on 8-inch centers. All personnel doors, except for the main entry, are considered emergency exits. These doors have no external hardware except for a key-way. The emergency exit doors are standard metal doors. The shipping/receiving area is physically separated from the manufacturing area. The main personnel entrance door is a standard plate glass door that opens into the access control area. After completing the initial access control and inspections, employees use their badges to open a steel door into the manufacturing area.

The storeroom is essentially a vault. The walls are 12-inches of reinforced concrete, and the door is equivalent to a class V vault door. The door is generally unlocked during operational hours and locked during the off-shift.

The manufacturing facility is connected to the site's central alarm station (CAS) through underground fiber-optic cable. The emergency exits and the main entry steel door are equipped with balanced magnetic switches (BMS) as is the storeroom vault door. The vault interior is equipped with microwave intrusion detection sensors to provide full coverage of potential access pathways.

The facility is staffed by a single, unarmed guard during operational hours only. The guard is equipped with a radio, telephone, and duress communications capability enunciating at the CAS. The site has an armed alarm response capability consisting of two 2-person teams equipped with semi-automatic rifles and handguns. The average response time to the manufacturing facility is 15 minutes. The CAS has direct radio communications with local law enforcement.

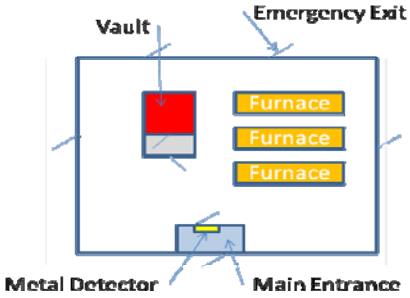


Figure D-1. Manufacturing Area

3. SCENARIOS.

a. Outsider Scenario 1: Dayshift – Armed Robbery. Nothing in the protection system is effective against this type of adversary action. The unarmed guard presents no threat to the adversary. The practice of keeping the vault door unlocked during day-shift operations significantly shortens the task time, even if the guard is able to activate the alarm. The adversary is able to get all the way into the vault with only minimal delay.

b. Outsider Scenario 2: Off-shift – Burglary. The building and door construction provide some level of delay to forcible entry. This, coupled with the BMS alarms on the entry doors, provides some degree of early detection. The vault walls and door provide approximately five minutes of delay and the vault alarms provide reasonable detection. However, the delay is shorter than the protective force response time, so the likelihood of adversary success is relatively high.

c. Insider Scenario 1: Abrupt Theft. There are two basic categories of insiders, those with direct access to bulk quantities of the material and those without. The vault custodian is the only adversary with direct access to bulk quantities of material. The vault custodian hides approximately 50 pounds or $1 million worth of material in his/her clothing and leaves the building at the end of his/her shift. There is nothing in the protection strategy to prevent this. The airport-style metal detector does not effectively detect platinum. There are no daily administrative checks of the status of the inventory.

d. Insider Scenario 2: Protracted Theft – Vault Custodian. Based on the results of the previous analysis, the result is approximately the same. As long as the theft is carried out between record audits, theoretically, the vault custodian could acquire the entire inventory.

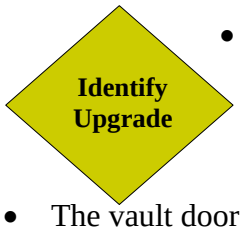
e. Insider Scenario 3: Protracted Theft – Production Worker. The production worker could attempt the same type of theft; however, the daily “take” is likely to be much less since he/she only has access to a small amount of the material on a daily basis, and if too much material is taken at once, his/her production rate would be affected. System effectiveness is significantly higher based on the material check in/out process.

Table D-1. High-Value Asset Path

Element	Detection	Delay
Daily Check out/in process	Low	N/A
Supervisor Check	Low	N/A
Monthly Records Audit	Low	N/A
Quarterly Inventory	Low	N/A
Emergency Exit Doors	N/A	15 seconds
Building Access Control	Moderate	N/A
Entry Door	N/A	15 seconds
Building Walls/Roof	N/A	4 minutes
Vault walls	N/A	5 minutes
Vault Door	N/A	5 minutes
Vault Alarms	High	N/A
Metal Detector	Low	N/A

4. UPGRADE OPTIONS.

a. Outsider. Options could include:



- An outer detection layer, such as an alarmed perimeter fence with both vehicle and personnel access controls, could provide some additional time against the dayshift robbery scenario.
- The vault door could be locked and the vault alarms activated at all times except when moving material in/out of the vault.
- Duress alarms could be placed in a number of areas inside the manufacturing area.
- Install a weight-monitoring system that keeps a real-time tally of the correct inventory weight and is tied to the CAS.

b. Insider. Options could include:

- Implement two-person control of the vault. This would help mitigate the risks associated with the vault custodian.
- Install metal detectors specifically designed to detect platinum at the access control point.
- Randomize the record audit process and inventories.
- Install a weight-monitoring system that keeps a real-time tally of the correct inventory weight and is tied to the CAS.

5. SUMMARY AND CONCLUSIONS.

This example is consistent with nearly all scenarios by revealing that protection against the insider is much more difficult to achieve than protection against the outsider. It is apparent that some actions can be taken to minimize the threat posed by both the outsider and insider. The analyst should always consider administrative procedures that can assist in the timely detection, if not prevention, of theft scenarios. Administrative procedures are often less expensive and provide reasonable assurance that the protection of the asset is sufficient.

The analyst can only provide the recommended upgrades to management. Management should then consider the cost benefit of the upgrades compared to the value of the asset, both short- and long-term. This is an ideal example of a risk management approach to a requirement that is not well defined.

APPENDIX E: PROTECTED AREA CONSTRUCTION

1. REQUIREMENTS. Numerous requirements are prescribed in DOE M 470.4-2, *Physical Protection*, Chapter IV.

2. SITUATION. A category II special nuclear material (SNM) site, Site Z *(fictional)*, is considering the construction of a new building within the protected area (PA). All SNM is stored in a compliant vault within the PA. Part of the PA fencing is being removed to accommodate the construction. Part of the existing PA fencing (two fences), vehicle barrier, and complementary alarms are being deactivated to accommodate the construction of a new building within the PA. A temporary PA boundary will be constructed to complete the PA boundary (see Figure E-1). The temporary PA boundary will consist of a single 7-foot fence with outriggers, a fence sensor, and a bi-static microwave sensor exterior to the fence. An animal fence will also be constructed to minimize nuisance alarms.

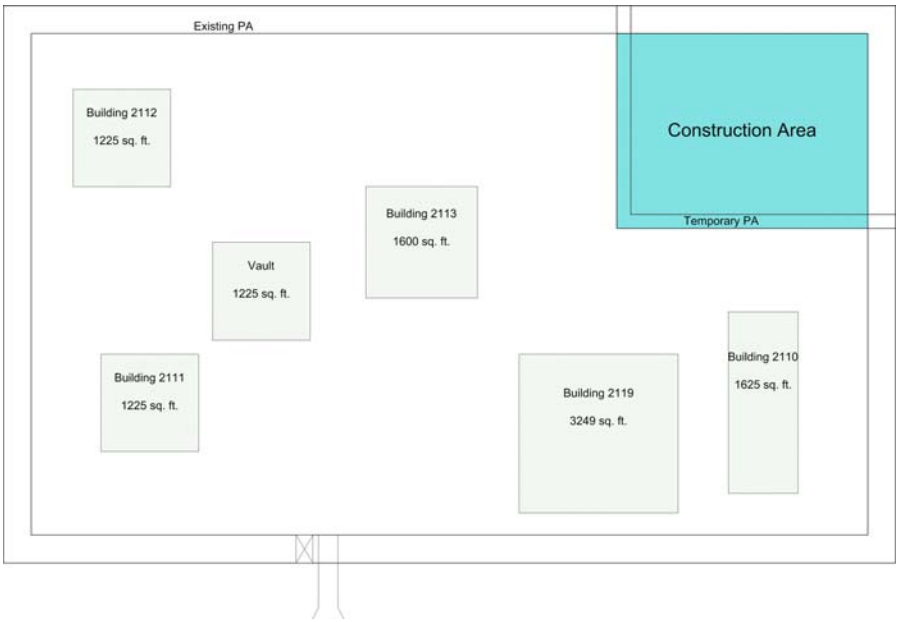


Figure E-1. Facility Layout

Define Target

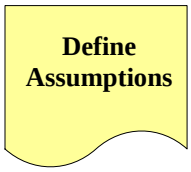
The target is a category II quantity of SNM. The SNM is stored within the PA in a compliant vault. All required access controls are in place. Armed protective force in available to respond to any alarms in a timely fashion. Alarms are monitored by a compliant central alarm station and a secondary alarm station. The target is vehicle-portable only and cannot be transported on foot.

(This threat definition is used for illustration. It does not necessarily reflect a threat derived from the Design Basis Threat (or subsequent replacement or relevant document)) The Design Basis Threat (or subsequent replacement or relevant document) defines the following adversary characteristics:

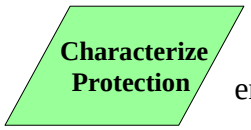
- Outsiders: Two individuals, each carrying an assault rifle. Transportation is a soft vehicle. Other tools include mechanical breaching tools.

- Insider: Not considered in this assessment.

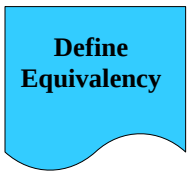
Note: So that the Guide may remain unclassified, the threat used in the examples may not correlate with the Design Basis Threat (or subsequent replacement or relevant document). However, when performing an actual analysis the current DOE threat guidance should be used.



The goal of the adversary is the theft of the category II SNM within the PA. All other elements of the protective system remain the same as before construction. This asset protection analysis will only compare the aspects of the temporary PA to the existing PA. The existing PA delay and detection is acceptable. The existing protective force response is adequate and unchanged during construction.



See Table E-1, Protection System Characterization – Site Z Temporary PA. This characterization is of the temporary PA employed during construction.



See Table E-2, Protection System Characterization – Site Z Existing PA. This characterization is of the existing PA.

Table E-1. Protection System Characterization – Site Z Temporary PA

Protection Element	Function	Effective Against	Compliant with Requirements	Comments
Fence				
- One 7-foot fence w/outriggers	Personnel Delay – 42 seconds[1]	Outsider	No	None.
Vehicle Barrier				
- Vehicle Barrier – interconnected "Jersey"	Vehicle Delay - 10 seconds[2]	Outsider	Yes	None.

[1] Sandia Barrier Handbook *(fictional value)*
[2] Sandia Barrier Handbook *(fictional value)*

Protection Element	Function	Effective Against	Compliant with Requirements	Comments
barriers				
Intrusion Detection				
Bi-static Microwave and Fence Sensor	Detection - P_D = 80%[1]	Outsider	No	None.
Protective Force				
- Posted PF	Detection - P_D = 50% Delay - 100 seconds[2]	Outsider	NA	PF will be posted 24/7 during construction.
- Random Roving PF Patrols	Detection - P_D = 20% Delay - 20 seconds[3]	Outsider	NA	Patrol frequency will be increased during construction hours.

Table E-2. Protection System Characterization – Site Z Existing PA

Protection Element	Function	Effective Against	Compliant with Requirements
Fence			
- Two 7-foot fences w/outriggers separated by 45 feet	Personnel Delay – 78 seconds[4]	Outsider	Yes
Vehicle Barrier			
- Vehicle Barrier – interconnected "Jersey" barriers	Vehicle Delay - 10 seconds[5]	Outsider	Yes
Intrusion Detection			
- Bi-static Microwave and Active Infrared	Detection - P_D = 90%[6]	Outsider	Yes
Protective Force			
- Random Roving PF Patrols	Detection - P_D = 20% Delay - 20 seconds[7]	Outsider	Yes

The existing PA provides 100 seconds delay and a P_D of 92%. The temporary PA provides 172 seconds of delay and a P_D of 92%. The comparison of these two figures shows that the temporary PA provides like and adequate protection compared to the existing PA.

3. UPGRADES.

Based on the above, no system enhancements are considered necessary.

---

[1] Site Z VA Group
[2] Sandia Barrier Handbook *(fictional values)*
[3] Sandia Barrier Handbook *(fictional values)*
[4] Sandia Barrier Handbook *(fictional value)*
[5] Sandia Barrier Handbook *(fictional value)*
[6] Site Z Testing
[7] Sandia Barrier Handbook *(fictional values)*

4. SUMMARY AND CONCLUSIONS.

The temporary PA provides at least equivalent protection to that of the existing PA. When comparing the various figures of merit; the existing PA provides 100 seconds of delay while the temporary PA provides 172 seconds of delay. It is noted that most of the temporary PA delay is provided by posted protective force which would be an additional cost borne during construction. It would be important that the construction be completed as soon as possible to minimize the extra cost of the posted protective force.

Table E-3. Summary of Results

Case	Existing PA	Temporary PA
Case 1	Compliant	Equivalent or better
Overall Rating	Compliant	Equivalent or better

FORMAT FOR THE ASSET PROTECTION ANALYSIS REPORT

1. INTRODUCTION.
   - *Facility/Location*
   - *Situation*
   - *Requirements*
2. DEFINE TARGET.
   - *Include the size and transportability of target being considered*
   - *Consider target conditions, configurations, associated task times and facility operations*
   - *Analysis should be applied to a specific target or location*
3. DEFINE THREAT.
   - *Should be consistent with the threat in the current Design Basis Threat (or subsequent replacement or relevant document)*
4. ASSUMPTIONS.
   - *Documented to include rationale for each assumption*
5. CHARACTERIZE PROTECTION.
   - *Security layers and boundaries*
   - *Applicable detection, delay and access controls*
   - *Include Protective Force response times whether armed or unarmed*
6. DEFINE EQUIVALENCY. *(when applicable)*
   - *DOE M 470.4-2, Physical Protection outlines vault type room requirements*
7. COMPARE PROTECTION.
   - *Describe how it is or is not equivalent*
8. IDENTIFY UPGRADES.
   - *Perform if comparison shows a lack of overall protection*
   - *Upgrades should show protection improvement*
9. RESULTS.
   - *Summarize the results and analysis conclusions*

SAMPLE REPORT

"Insert Classification Determination throughout Document"

Asset Protection Analysis for Confidential Matter Stored in a Limited Area.

(Not in Compliance with DOE M 470.4-4, Information Security)

1. INTRODUCTION. The following is an analysis of the protection measures provided for a classified device located in a limited area (LA). The device, a radar system, is classified at the Confidential level. While the LA does not meet all of the protection requirements, it was determined to provide equivalent protection. Possible upgrades include locking the device in a cabinet. *The threat characteristics depicted and the example are fictitious and do not represent the Department threat guidance or an actual facility situation.*

   DOE M 470.4-4, *INFORMATION SECURITY*, CHAPTER III-3, REQUIREMENTS FOR STORAGE OF CONFIDENTIAL MATTER.

   - In a locked vault (requirements for vaults are included in DOE M 470.4-2, *Physical Protection*) or in a locked General Services Administration (GSA)-approved security container within an LA or higher.

   - In a locked vault-type room (VTR) (requirements for VTRs are included in DOE M 470.4-2, *Physical Protection)* within an LA, exclusion area (EA), protected area (PA), or material access area (MAA) equipped with intrusion detection system (IDS) protection. The protective forces (PF) must respond within 30 minutes of alarm annunciation.

   - When located outside an LA, the locked vault or VTR must be under IDS protection. The PF must respond within 15 minutes of alarm annunciation.

   - In locked, steel filing cabinets that do not meet GSA requirements (containers purchased and approved for use before July 15, 1994 and may continue to be used until October 1, 2012) and are equipped with three-position, dial-type, and changeable combination locks. The cabinet must be in a locked area or building within the minimum of an LA, EA, PA, or MAA.

2. DEFINE TARGET. The target is a piece of sensitive electronic equipment classified as Confidential. The equipment is a radar unit used to detect elements entering and moving within a perimeter intrusion detection assessment system (PIDAS). The radar unit measures approximately 1.5 feet x 1.5 feet x 2.0 feet. It is person-portable and weighs less than 50 pounds. It is housed in a case with a carry handle on top.

3. DEFINE THREAT.
   Outsiders: One individual. Tools include mechanical breaching tools.

4. ASSUMPTIONS.

- Thieves want to steal the equipment for exploitation and study.
- Assume there are two threat scenarios:
  - An outsider, working alone, gains access to the PPA after hours (primarily unchallenged, but still detected) and is able to locate the LA and force entry. The outsider steals equipment and is able to escape.
  - The outsider is working with an insider to gain entry to the PPA. The outsider and insider force entry into the LA, steal the equipment, and escape before PF personnel arrive.
- The insider will have access to the PPA only, not the LA.
- Assume that, on average, it takes PF personnel 10 minutes to respond to an alarm after dispatch from the central alarm station (CAS).

Assume the LA meets all requirements, and all alarms function correctly.

5. CHARACTERIZE PROTECTION. The target is located in room 14 within an LA in the Germantown Building (see Figure 1).

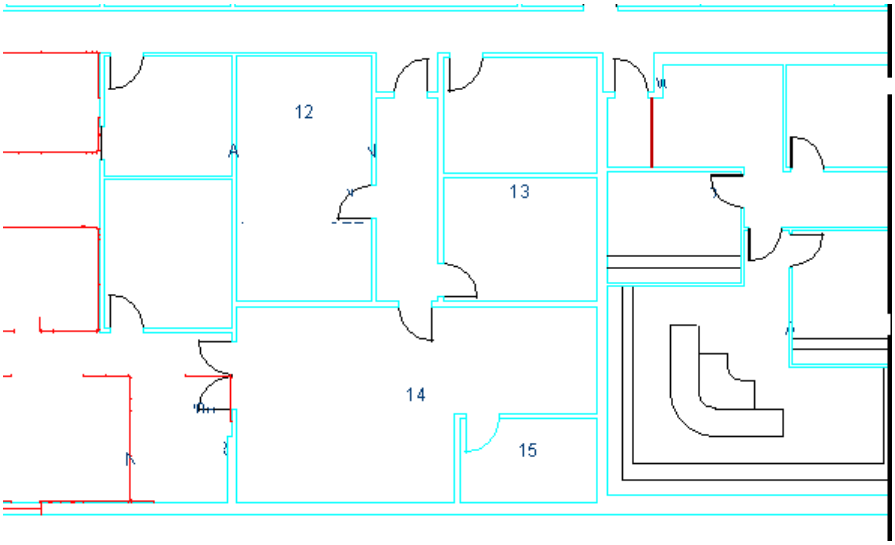


Figure 1. Limited Area, Germantown Building

The LA is surrounded on two sides by a PPA, by a security area on one side, and the other side is an exterior building wall (cinder block construction, no windows). Access to the PPA is controlled by a card reader. “Piggybacking” into the PPA is permitted provided that the individual allowing access has verified that all individuals entering have an approved U.S. Department of Energy (DOE) badge. The PPA doors are alarmed with balanced magnetic switches (BMS).

The LA comprises four rooms and a hallway/vestibule. The entry door is controlled by a card reader (a personal identification number [PIN] is also required to gain access) and is alarmed with a BMS. The rooms to the east and west, rooms 12 and 13, are offices and are not alarmed. The main south room, room 14, is where the target is stored. The entry door to room 14 is alarmed with a BMS. Room 14 also has two emergency exit doors that exit into the PPA. Both doors are alarmed with BMS units. There are ceiling-mounted motion detectors providing 360 degree coverage for the majority of room 14. The walls are floor to "virtual ceiling," meaning there is a space between the top of the wall and the ceiling but it is too small for a person to gain access. The floor is a false floor, but the space between the false floor and the true floor is less that 1 foot. When the room is occupied, the area is placed in "access" (i.e., the BMS on the main entry and on room 14 along with the motion detectors are shunted).

6. DEFINE EQUIVALENCY. Since the item cannot be stored in a GSA Security Container equivalency would require storage in a vault-type room as outlined in the requirements in the introduction above.

7. COMPARE PROTECTION.

   a. Outsider Acting Alone – Item in LA. In this scenario, the outsider is able to gain access to the PPA with minimal effort but there is evidence of intrusion at the PPA. (Detection could occur at this time, but in this case, it is assumed the adversary is not detected.) The outsider is able to locate the LA but is not able to gain access without evidence of intrusion. The outsider gains access to the LA. Upon entry, the adversary is detected by the motion detectors, which initiate a response. The outsider obtains the classified device and attempts to flee the area before PF personnel arrive at the scene.

   b. Outsider Acting Alone – Item in VTR. In this scenario, the outsider is able to gain access to the PPA with minimal effort but there is evidence of intrusion at the PPA. (Detection could occur at this time, but in this case, it is assumed that the adversary is not detected.) The outsider is able to locate the VTR but is not able to gain access without evidence of intrusion. The outsider gains access to the VTR. Upon entry, the adversary is detected, and a response is initiated. The outsider obtains the classified device and attempts to flee the area before PF personnel arrive at the scene.

   c. Outsider Acting in Cooperation with an Insider – Item in LA. An outsider is given access to the PPA and led to the LA without detection. The insider does not have access to the LA; therefore, there will be evidence of intrusion. The outsider and/or insider gain access to the LA. Upon entry, the adversary is detected by the motion detectors, which initiate a response. The outsider obtains the classified device and attempts to flee the area before PF personnel arrive at the scene.

   d. Outsider Acting in Cooperation with an Insider – Item in VTR. An outsider is given access to the PPA and led to the VTR without detection. The insider does not have access to the VTR; therefore, there will be evidence of intrusion. The

outsider and/or insider gain access to the VTR. Upon entry, the adversary is detected, and a response is initiated. The outsider obtains the classified device and attempts to flee the area before PF personnel arrive at the scene.

e. Insider Acting Alone – Item in LA. The insider has access to the PPA and can move to the LA without detection. The insider does not have access to the LA; therefore, there will be evidence of intrusion. The insider gains access to the LA and, upon entry, is detected by the motion detectors, which initiate a response. The insider obtains the classified device and attempts to flee the area before PF personnel arrive at the scene.

f. Insider Acting Alone – Item in VTR. The insider has access to the PPA and can move to the VTR without detection. The insider does not have access to the VTR; therefore, there will be evidence of intrusion. The insider gains access to the VTR and, upon entry, is detected by the motion detectors, which initiate a response. The insider obtains the classified device and attempts to flee the area before the PF personnel arrive at the scene.

8. IDENTIFY UPGRADES. Place equipment, when not in use, out of sight in a locked file cabinet or similar storage.

9. RESULTS. The target is provided protection equivalent to compliant protection of Confidential classified matter. If the target is being stored for a short-term period of time, no upgrades or additional protection would be needed. If the storage of the target is long term, additional protection may be prudent, such as placing the target, when not in use, in a locked cabinet.

Case	Vault-Type Room	Limited Area
Outsider Working Alone	Compliant	Equivalent
Outsider Working With Insider	Compliant	Equivalent
Insider Acting Alone	Compliant	Equivalent