SAND2016-0225R

Prepared For Lithuania Radiation Protection Center
January, 2016

Regulatory Guidelines on Conducting a Security Vulnerability Assessment

Prepared by
Sandia National Laboratories
Albuquerque, New Mexico 87185 and Livermore, California 94550

Sandia National Laboratories is a multi-program laboratory managed and operated by Sandia Corporation, a wholly owned subsidiary of Lockheed Martin Corporation, for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-AC04-94AL85000.

For use by Radiation Protection Center, Lithuania.

Regulatory Guidelines on Conducting a Security Vulnerability Assessment

Purpose of Regulatory Guidelines

This document will provide guidelines on conducting a security vulnerability assessment at a facility regulated by the Radiation Protection Centre. The guidelines provide a performance approach assess security effectiveness. The guidelines provide guidance for a review following the objectives outlined in IAEA NSS#11 for Category 1, 2, & 3 sources.

Background:

A vulnerability assessment is a method for evaluating protective security systems. This method can be used both by the operator and by RSC to measure the security system effectiveness and to identify any potential security vulnerabilities that should be addressed. It is used to confirm that the performance of the security program effectively meets the regulatory security requirements by identifying weaknesses in the security system that could be exploited by the DBT adversary.

For this document to be effective, it is important that the DBT be a part of the regulatory documentation. Further, a requirement for a Vulnerability Assessment should be established in the regulations. It is assumed that this requirement and the subsequent level measures are consistent with NSS #11.

The intent of the vulnerability assessment is to validate the manner in which the prescriptive security measures were applied. In developing this guide, a graded approach was applied to the vulnerability assessment, whereby a more robust vulnerability assessment approach was applied to more attractive materials.

The document achieves this by:

1. Providing confidence that the detection measures installed will, in fact, provide intrusion detection of the DBT-like adversary. It does this by confirming that no security gaps exist in the concentric security layers surrounding the targets, and conducting tests to confirm that the sensors are operating correctly. This detection includes insider detection. This is done for categories 1, 2, and 3 materials.
2. Providing confidence that there are no gaps in the concentric layers of barrier. This is done for categories 1, 2, and 3 materials.
3. Providing assurance that the two concentric barrier layers are composed of barrier measures that are substantive. This is done for categories 1 and 2 materials.

4. Providing confidence that there are adequate and redundant communications between the site and the response forces, and conducting tests to this end. This is done for categories 1 and 2 materials.
5. Providing confidence that the security measures in place will permit an effective and timely response by conducting a tabletop exercise on a periodic basis. This is done for category 1 materials.

Basis for the Vulnerability Assessment:

The vulnerability assessment should be based upon the national security regulations, including the Design Basis Threat established by the RSC.

When is a Vulnerability Assessment Conducted

The vulnerability assessment should be conducted initially in order to confirm the planned security system will achieve its required objectives prior to the submission of the initial site Security Plan. This vulnerability assessment will be repeated by RSC when reviewing and approving the plan.

The vulnerability assessment should be repeated and updated annually to ensure that security system effectiveness is maintained, and to identify any new vulnerability.

A vulnerability assessment (VA) should be considered as part of each regulatory inspection. This can draw from previous vulnerability assessments or confirm that the security system outlined in the approved security plan will effectively mitigate the risks posed by the DBT. For the former, the review will review the previous vulnerability assessment and ensure it applies to the current security system. For the latter, the VA will confirm that the security plan accurately represents the existing security system.

Prior to Conducting a Vulnerability Assessment

In preparation for conducting a vulnerability assessment, a review of the security regulations, the DBT, the license (to identify the sources, activity, and uses), the facility security plan, previous vulnerability assessments of the facility, and any reported security incidents to the regulator should be made. Confirm the category of the radioactive sources in the inventory, and understand that expected transportation/movement of sources. As appropriate, confirm assumptions used in previous vulnerability assessments.

Conducting the Initial Vulnerability Assessment

The vulnerability assessment will endeavor to identify security vulnerabilities by a thorough, performance-based review of the security system with respect to the regulations and the DBT. The review will be achieved by: 1) verifying that no gaps exist in the detection of the malicious acts by the DBT (including access control) and that security layer barriers are continuous; 2) Assessing the effectiveness of security programs against insiders; and 3) verifying the response effectiveness (including the delay effectiveness) to the malicious acts by the DBT. The approach for each of these is described in the succeeding sections.

1.0 Identify Layers of Security

1. Obtain a site layout and floor plan of each building of concern (i.e. buildings containing sources or other security-important buildings within the site). Annotate on floor plans the location of radioactive materials, alarm station, guard locations, response force locations and any other features that will influence security effectiveness. Use existing security plans, and discussions with site personnel to complete this.
2. Outline security layers that envelope the source. A security layer[1] is a continuous boundary of detection and delay measures that envelopes a radioactive source (e.g. a perimeter fence, including detection measures, that surrounds the entire campus). The site security manager should be able to identify these.
    a. Follow continuous physical boundaries (walls, fences, doors, etc.) that define security layers. Using highlighter, follow the boundary of each security layer on the drawing (note any gaps in physical boundary—openings that cannot close—that constitute the continuous layer surrounding the radioactive material).
    b. Identify all access points across the layer, including emergency access. This includes all doors and gates.

2.0 Verifying no gaps in detection (Source of Category 1, 2, & 3)

Objective: to confirm that layers of security are established in which barriers continuously (no gaps) surround targets, and that intrusion attempts across the layer at any point is subject to detection.

Assess Detection Gaps in Layers

a. Intrusion

- Identify detection of penetration along the layer[2]. These could be door sensors, vibration sensors, glass break sensors, or infrared/microwave sensors. They could be people posted to provide surveillance or remote surveillance using CCTV. Detection could also be provided by staff working in the area that would call security, but this should only be considered if staff have a specific documented responsibility to provide surveillance and the staff on been trained to do this.

  On the layout drawing, note each detection method for a layer[3]. Any boundary segments (walls, doors, windows, etc.) without detection to penetration should be noted. ***Any boundary segment through which the DBT can penetrate without detection would be a potential gap and should be noted.*** (Note:

[1] A security layer could be a the walls of a safe (which encompasses a source), or it could be a the surface of a room (4 walls, ceiling, floor, doors), or it could be a building surface, etc.

[2] Detection is always associated with a layer, but the converse is not necessarily true: a layer of barriers does not necessarily have to include detection (although it should). Generally when two layers are implemented, detection is emphasized on the outer layer (as detection precedes delay), but could also be on the inner layer (since access control on a layer without detection is not very effective).

[3] Identify any detection measures or access controlled entries not associated with a layer. This could be flagged to be moved onto a layer as their value may be questionable. (Volumetric sensors are usually installed just inside or outside of a layer boundary, and are associated with these layers.)

Barriers that are deemed impenetrable to the DBT adversary do not require any detection methods and are not considered vulnerabilities.)

Check installation/condition of sensors and cameras. Check if sensors and cameras are oriented to detect/see what is intended.

Any detection method that depends entirely on a single person being observant and reporting a malicious action may be a weak point in detection and should be tested covertly.

- Identify how detection is assessed (e.g. cameras, guards, patrols, etc). If assessed by guards/patrols, where are the guards/patrols coming from? Are there written procedures for how to assess alarms (given that guards will likely be too late to observe adversary causing alarm)? If there is no reliable means defined, then assessment is not reliable. ***Any detection method that is not accompanied by an effective assessment means is a potential gap and should be noted.***
- Conduct simple functional test of sensors (can they detect?) and cameras (are images transmitted/light sufficient?). To do this, you need to be in communication with the alarm center to confirm that alarms are properly received. ***Any sensors that fail to detect or cameras do not permit assessment constitute a potential gap in detection and should be noted.***
- Identify when the alarms are in active mode (armed) and when they are inactive (disarmed). It is common that the alarms are disarmed during operations to prevent continuous alarming. Identify how alarms are armed/disarmed. Confirm that unauthorized persons cannot disarm alarms. Methods to achieve this are: to require secret code to disable alarms, or require two different people disable alarms. If code, ensure code is not universal (everyone uses the same code) and that code is protected. If two persons, ensure that a single person cannot covertly deceive the system. **Any scenario in which a single insider person can disable alarms, without an immediate alarm, constitutes a vulnerability.**
- Identify what detection measure (usually people) are in place to compensate when sensors are disarmed. Confirm written procedures that instruct personnel what to look for and how to report it. ***Any alarms that are disabled without corresponding compensatory detection measures constitute a potential gap and should be noted.***

b. Alarm Monitoring and Communication

- Verify that the monitoring station is staffed continuously. Investigate how alarm station remains staffed during personal need breaks, and during emergency situations. If alarm station is not monitored 24/7, how are alarms

monitored/who do people call if they notice irregularities? ***Alarms that are not monitored continuously constitutes a potential gap and should be noted.***

- Verify that the alarm station is locked and provided adequate protection from the DBT. An alarm monitoring station that is not locked and protected could be the target of attack to prevent alarms from being communicated. ***As such, a monitoring station that is not protected and locked constitutes and potential gap and should be noted.***
- Verify that the station possess redundant communications to the response forces (for category 1 and 2 only). Redundant implies two different paths, but this is improved if it is also two different technologies. (landline phone, mobile phone, radio, etc). ***Note any issues or discrepancies.***
- Confirm that there are written procedures to be followed when communicating with response forces. Test communications with a drill, alerting response forces. ***Note any issues.***

c. Access Control

- For each access point (e.g. doors) on a security layer, note how and when access is controlled (keys, badges, etc. for both working and non-working hours). What are procedures for access (show badge? Obtain key and unlock door? No procedures)? ***Doors without access control (locks) are considered barrier gaps in the security layer***. These doors provide no delay to an adversary, even if they are alarmed.
- For adversary with DBT capabilities, identify measures to detect adversary activities, such as: unauthorized making or obtaining keys or badges, overpowering or deceiving guard into permitting entry, etc. ***An absence of detection measures for any of the above constitute a vulnerability and should be noted.*** A detection measure can be sensors, surveillance by dedicated persons, or remote surveillance.

Access control should provide confidence that an unauthorized person cannot enter undetected? *If this is not the case****, the access control measure represents a vulnerability.***

Identify Insider Protection (If DBT includes active insiders)

Objective: To determine if there is a likelihood of detecting insiders.

1. Identify trustworthiness programs in preventing insider. These programs would include:
   a. investigations performed during hiring,
   b. periodic re-investigations,
   c. insider awareness training for staff

   Investigations strength is based on the breadth and depth of subjects investigated, including identify verification, criminal history, psychological health, financial health, medical addictions, and any other issues that could make one vulnerable to blackmail.

A graded approach to trustworthiness should be employed, where persons with unescorted access to highest category materials should be subjected to the most rigorous checks. Identify what policy is in place for trustworthiness checks, and what level of rigor is applied to different insider groups. Confirm records of checks for current staff to confirm checks were done.

Persons with access to or authority over radioactive sources who have not been subjected to background checks represent a vulnerability.

2. Identify how insiders are mitigated[4]
    a. For the following types of insiders, identify insider mitigating measures to prevent a malicious act:
        i. Management (non-operator personnel with authority)
        ii. Operators (e.g. doctors, nurses, technicians, etc)
        iii. Maintenance personnel (repair persons, janitors, etc)
        iv. Security Staff (guards, firefighters, etc)
    b. The following areas should be addressed for insiders detection and access:
        i. The security layers
        ii. Immediate Target
        iii. Guard station
        iv. Alarm/video monitoring center
        v. Badging/Key storage area
    c. Identify detection of insider groups. For each group, assess possible detection through:
        i. Intrusion sensors described above, if they are active and will alarm on the insiders.
        ii. Tamper seals, assuming insider cannot by-pass or defeat
        iii. Co-worker surveillance so long as there are written procedures instructing oversight (escorts, two-person rules, continuous active surveillance, etc), or it is impossible for an insider to be alone (two-person locks) and all workers receive training on how to surveil co-workers for inappropriate behavior.
        iv. Contraband detection, if contraband is required to perform malicious act. Contraband items and searches must be included in written procedures. Contraband can include:
            - weapons
            - tools for breaching
            - explosives

        Note insider groups for which no insider detection exists.

    d. Identify access permissions and restrictions for the insider groups. Identify where and when the insider groups are permitted entry. Also, list any restrictions, e.g., need for escorts, two-person control that any groups have.
        i. Note insider groups that have no access limitations.

[4] This section is skipped if trustworthiness is credited.

e. Identify authorities of insiders. Specifically, can insiders approve/modify access permissions to sensitive areas; can insiders approve movement or shipment of sources; can insiders dictate security levels applied to sources (e.g., change surveillance, or disable alarms).

f. Review list insiders without detection and list of insiders without access controls to targets. ***Insider groups for which both no insider detection exists and no access limitations are in place constitute a serious potential vulnerability and should be noted.*** These insiders should be subject to the most stringent trustworthiness checks. Efforts should be met to reduce access and/or provide surveillance for these insider groups.
Further, consideration should be given to provide detection for insiders with no detection (but already are subject to access limitations); and to provide access limits for insiders with no access limitations (but already are subject to detection).

g. Review list of insiders with authorities over target materials or target material security. ***Insider groups that possess unchecked/unchallenged authority to move sources or disable detection systems constitute a serious potential vulnerability and should be noted.*** These insiders should be subject to the most stringent trustworthiness checks. Efforts should be met to divide authority so that no single person can remove security from sources or approve shipment of a source.

3.0 Verifying no gaps in Barriers (Categories 1, 2, and 3)

Assess Barrier Gaps in Layers

2. Walk-down facility to observe the layers and components highlighted on the layout. Walk-down should be conducted with site security personnel. The walk-down should:
    a. Confirm continuity of each security layer and look for holes in layer barriers or other differences from the layout drawing. Make appropriate changes to drawing.
    b. Provide further information on delay
        - Confirm identity of different types of barriers (e.g. doors, walls, ceiling, windows, etc)
        - Characterize robustness of barriers (for cat 1 materials only)
            1. Doors: *wooden* vs *steel*, *hollow* vs *solid*, *double* vs *single*; *sliding* vs *swinging*;
            2. Hinges: *light* vs *heavy duty*, *Pin or hinge accessible from outside* vs *inaccessible*,
            3. Walls: *brick* vs *plaster board* vs *reinforced concrete*
            4. Windows: *plain glass* vs *glass with wire embedded* vs *glass with security film* vs *glass with bars*
            5. Locks: *keyed cylinder* vs *dead bolt* vs *electric strike* vs *magnetic*

For Category 1 and 2 materials:

- Check condition of barrier segments (walls, ceiling, floors, doors, windows). Note any issues with installation or maintenance.
- Identify weak barriers in mandated layers intended to provide delay[5]. ***Any gap in continuous layer of barriers, or any weakness in a barrier segment may constitute a vulnerability and should be noted.*** A weak barrier segment would include:
    1. plain glass windows without bars or other hardening,
    2. plaster board walls or other construction that can be quickly breached with hammer, axe, or other non-powered instrument,
    3. large vents or air conditioners that could permit easy passage.
    4. simple door locks (no deadbolt) into wooden door jams,
    5. hollow wooden doors.

3.0 Response and Delay Effectiveness: (Category 1 and 2)[6]

Assessing Timeliness of Response Force Interruption and the Ability to Stop the Progression: Tabletop Exercise (Sources of Category 1)

The results of a recent tabletop exercise should be used as the basis for the assessment of the response force ability to interrupt and stop the detected adversary. The tabletop should be conducted on the facility, taking into account the security measures (including expected delay these measures present to the adversary). The tabletop should include: facility security staff, guards, on-site response force, operators of the radioactive materials, site management, and other emergency personnel; local off-site responding organizations and off-site monitoring personnel; local and national law enforcement organizations; and local fire and other emergency personnel.

A following should be established prior to the start of the tabletop:

- the types of scenarios to be assessed in the tabletop (theft, sabotage, targets)
- the DBT adversary characteristics to be exercised
- the layer of assumed detection for the scenarios
- the delay times offered by the barriers[7]

---

[5] Category 1 and 2 sources require two concentric layers of barriers. Category 3 sources require one layer. Access Control is always associated with the layer.

[6] The tabletop should be repeated on a regular basis: for category 1 radioactive material, a tabletop should be completed every two years; for category 2 material, a tabletop is recommended be completed every 5 years. The objective of the tabletop for category 1 sources is to confirm that response is timely and of sufficient strength to stop the adversary. The objective of the tabletop for category 2 sources is to confirm that the response is generally timely.

- the task time for the actual malicious act[8]
- the assumed staffing and specific location of patrols (law enforcement, security, and other responders) during: daytime operations, nighttime operations, and holiday operations
- the rules of engagement
- the protocol for communication, and time for alarm assessment and communication to alarm station and from alarm station to response force
- the movement rates for adversary and responders during daytime, nighttime and holiday.

The tabletop should be structured and conducted employing an independent facilitator to oversee the run the exercise. See the Annex 1 for details on the conducting a tabletop exercise.

4.0 Resolving Issues Identified in the Tabletop.

This section provides an approach to combine the results of the VA and provide corrective actions.

1. Assemble all noted gaps in Detection. Each gap must be addressed either by introduction of new or repaired detection equipment or new detection procedures. Compensating measures should be defined to address vulnerability until a final solution is in place.
2. Assemble the noted gaps in delay on required layers. In particular, any plain glass windows, unhardened vents with man-sized openings, or soft walls/ceilings/doors[9] shall be compensated for.
3. Assemble all noted insider gaps and vulnerabilities. Each vulnerability must be addressed with an appropriate solution that prevents a single insider from having the access and/or authority to facilitate a malicious act. Solutions could include:
   For access vulnerabilities,
   - Surveillance,
   - Two-person controls or
   - compartmentalizing access;

   For authority vulnerabilities,
   - requirement for two or more people approve any change in material or security prior to implementing a change or initiating a move.

4. For Category 1 sources, list gaps and vulnerabilities identified in the tabletop. In particular with regards to response timeliness, solutions must be developed to counter the vulnerability. Solutions to address inadequate delay should include improved barriers. Solutions to address

---

[7] The assumed delay times of barriers will have significant impact on timeliness and so some effort should be taken to develop confident estimates. This would include gathering input on the fire and police experts in breaching barriers. Do not use the fastest or slowest possible breach times, but the most realistic times.

[8] Same as above. Base this on the specific tasks that an adversary must perform.

[9] A soft wall, ceiling or door is defined as a surface through which a man-sized hole can be created quickly using light hand tools (e.g. hammer). A masonry board wall, a hollow wood-particle board door, or a suspended acoustic tile ceiling would be examples of such light barriers.

insufficient responsiveness need to be developed and implemented. These might include formal memorandums of Understanding between response organizations and the site, facility Target Folders developed to facilitate off-site response force familiarity with the facility, and active programs to lengthen the adversary time (e.g. removing power, barricading doors or blocking vehicle exits when an adversary is known to be engaged in a malicious act).

5. Assemble all noted vulnerabilities from the tabletop. Develop solutions to each. A plan for implementing identified solutions, including securing resources for their implementation, developing a realistic schedule for their implementation, and identifying compensatory measures to be implemented until the solutions are implemented.