A DIVISION OF NERC

E-ISAC

ELECTRICITY INFORMATION SHARING AND ANALYSIS CENTER

Vulnerability of Integrated Security Analysis: Implementation Guide

TLP:GREEN

RELIABILITY | RESILIENCE | SECURITY




1401 H Street NW
Suite 410
Washington, DC 20005
202-790-6000 | www.eisac.com

Table of Contents

Executive Summary

Vulnerability of Integrated Security Analysis (VISA) is the result of a nationwide competition to develop a standard vulnerability assessment method to be used at licensed nuclear facilities in the United States. The VISA method was first presented at the 1977 Institute of Nuclear Materials Management annual meeting by Science Applications International Corporation (SAIC). This vulnerability assessment methodology has been applied to high-risk government facilities for decades. Through the years, the method was refined, and the process was again presented to the Institute of Nuclear Materials Management annual meeting in 1992. The VISA tabletop methodology is scenario-based and uses a group of subject matter experts from different disciplines (e.g., physical protection, cybersecurity, nuclear material control, accounting, protective force, and transportation) to logically develop and evaluate scenarios.

VISA is simple to use and flexible because users can apply it to all types of facilities and systems, and it addresses all types of threats and targets for both insiders and outsiders. VISA can be based on documented values (i.e., performance testing results, pre-established tables of probabilities, equipment specifications), professional judgment, or a combination of both. One weakness of the process is that the quality of the results depends heavily on the capabilities of the subject matter experts involved in the process. However, the transparency of the process readily allows for quality control reviews. VISA is an intuitive approach using a logical process and application of critical subject matter expertise throughout.

In 2015, the Electricity Information Sharing and Analysis Center (E-ISAC) Physical Security Advisory Group (PSAG) developed the Design Basis Threat (DBT) document to assist asset owners and operators (AOOs) in assessing the physical security of the bulk power system. A DBT is defined as follows:

> *The threat against which an asset must be protected and upon which the protective system's design is based. It is the baseline type and size of threat that buildings or other structures are designed to withstand. The DBT includes the tactics aggressors will use against the asset and the tools, weapons, and explosives employed in these tactics.*[1] *Furthermore, a DBT is derived from credible intelligence information and other data concerning threats but is not intended to be a statement about actual, prevailing threats*.[2]

To further assist Asset Owners and Operators (AOOs) the PSAG requested the U.S. Department of Energy (DOE), Office of Infrastructure Security and Energy Reliability to develop an implementation guide. As part of their commitment and support to the PSAG, DOE's Pacific Northwest National Laboratory (PNNL) created this guide that provides one possible approach for companies or utilities to use in assessing their physical protection systems (PPS) and the response to a site and/or asset.

Although many other tools and approaches exist to assess the effectiveness of a PPS, the PSAG selected the DBT approach as an organization's physical security subject matter experts (SME) can use it relatively inexpensively, reasonably quickly, and without outside assistance. This approach yields actionable results that can be either quantitatively or qualitatively defined and provides a sound basis for risk acceptance or upgrade investments.

This guide uses the VISA process to show vulnerability assessment practitioners how to implement a DBT. The VISA methodology is one of many risk assessment tools that can use a specified DBT to determine the overall system effectiveness of an integrated PPS. VISA is a cost-effective methodology relying on SME input to help determine overall system effectiveness.

[1] JP 1-02. SOURCE: JP 3-07.2 *Department of Defense Dictionary of Military and Associated Terms*

[2] International Atomic Energy Agency DBT Terminology

Notice of Modifications

Background

- PSAG first developed a document in 2015.
- Published in February 2017 by PNNL on behalf of DOE.
- Revised in May 2019 (contains minor formatting and graphic updates, but no substantial changes in methodology).
- Revised in June 2020 (contains updates based on the latest revisions made by PNNL to their "User Guide to the VISA Tool and Methodology").
- Revised June 2021 (contains updates to the step scores based on feedback received during the VISA Facilitator's course in April 2021) and a revised definition of a design basis threat.
- Revised in August 2023 to incorporate changes and updates to improve user efficiency and incorporate lessons learned through the VISA workshop. A major addition was the updating of an updated insider threat scenario and a clarification on detection and assessment.
- A copy of the original document is available on the E-ISAC Portal.

Chapter 1: System Effectiveness Analysis

This chapter is intended to provide an overview of the System Effective Analysis (SEA) Team and how their subject matter expertise is critical throughout the Analysis Process.

System Effectiveness Analysis Team

When putting together a SEA team, it's critical to establish a core support team with the applicable subject matter expertise (SME). Team member selection should be based on experience and the willingness to work in a team environment towards a common goal.

The core team should consist of the following members:

- A representative from Operations who has a detailed understanding of the function of the site and its critical components
- A representative from grid operations
- A representative from the security operations centre (if there is one)
- A representative from IT/OT, including networks
- A representative from Human Resources
- A SEA analyst or security systems/operations specialist
- A PPS SME familiar with the PPS system and any other interconnected systems
- A cybersecurity SME who is familiar with the site layout and the PPS communication protocols. This member must be different than an Information Technology [IT] person
- An onsite security supervisor or those having responsibility for the overall security posture of the facility
- An off-site response representative or local law enforcement

The core SEA team is responsible for gathering all the necessary information before it begins its analysis. This information would typically include the following:

- Google Earth images
- Floorplans with the location of all the detection systems, cameras, doors, walls, gates, etc.
- Both on-site and off-site response plans, including any communication links with local law enforcement
- Any documented physical security and response procedures
- Accurate day/night response times for all responders
- Current site security plans

During the actual scenarios, the SEA analyst will represent the adversary's actions, and the facility or site security manager will represent the actions of the PPS and responders. Any digital attacks or electronic responses are normally handled by the cybersecurity SME.

The System Effectiveness Analysis Process

The *Vulnerability of Integrated Security Analysis (VISA) Implementation Guide* frames a process by which physical security experts in utilities can assess the effectiveness of their facility's protection systems based on current reasonable and credible threat considerations. In this report, the term "system" refers to the facility's overall physical protection system (PPS), including the response. The system effectiveness analysis (SEA) is a standard sequence of steps to evaluate system effectiveness regardless of the analysis methodology. Detection, assessment, delay, and response are evaluated as part of the process, shown in **Figure 1.1**. The VISA methodology is a good fit for conducting analysis within the bulk power system because it is a scalable, low-cost self-assessment tool with a high impact for security managers.

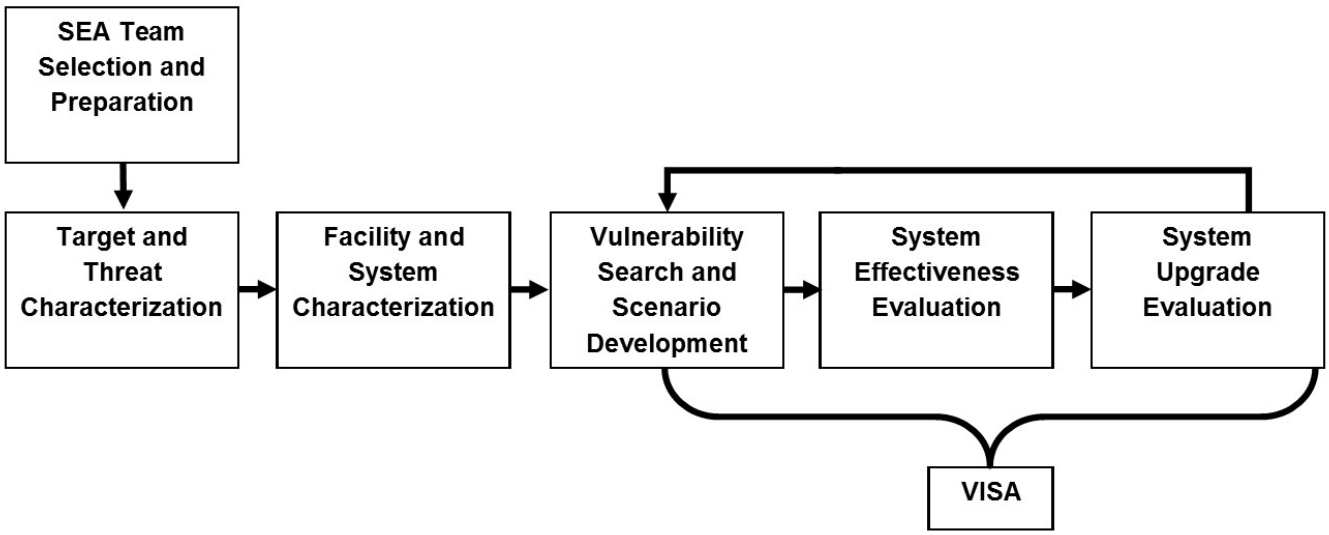

Figure 1: System Effectiveness Analysis Process

Chapter 2: Site Details

This chapter provides an overview of site-specific considerations that should be taken into account prior to selecting a facility, site, and or target. This chapter also provides examples of the primary components of a Physical Protection System (PPS), furthermore, how each function can be broken down into further detail.

Site Characterization

Thoroughly understanding all aspects of the site's detection, assessment, delay, and response capabilities is critical. Any systems that operate or support the Physical Protection System (PPS) should be examined. This includes the site location, as well as daytime versus nighttime operating conditions. The goal is to determine the asset protection level (APL) for the site or target so an appropriate level of DBT can be applied. The APL is further described in *Chapter 1 of the Electricity Design Basis Threat*.

For example, if a specific transformer site or control station is deemed critical to the Bulk Power System or the asset owner/operator, it should be classified as APL 1. In the analysis phase, the team should document target descriptions and include photographs, if possible. Characterizing the target or specific critical components can involve many different activities, from information gathering to actual site tours. The team should also document adversary pathways, any dedicated response positions (i.e., guard booths), and times for responders. Failure to adequately characterize a facility can lead to inadequate or overly restrictive security being applied, including failure to sufficiently protect a facility.

Target Prioritization

High-consequence target or component descriptions should be documented and include photographs (if possible), for the analysis phase. Characterizing the target or specific critical components can involve many different activities, from information gathering to actual site tours. When reviewing targets or assets at a facility, the team should use a graded protection strategy as a norm. Simply put, the most attractive or critical targets to an adversary should require the most protection and coverage from the PPS. Conversely, the least attractive target should have a lesser degree of protection.

Facility or Site Characterization

Understanding all aspects of the site's detection, delay, and response capabilities is critical. The team should examine any system that operates or supports the PPS. The team should also document the response time including various security conditions and examine facility or site operating procedures and any digital control systems that automate or integrate the PPS. Any assumptions made, the core SEA team must document and then validate with the appropriate person or agency.

This activity is best done on the site itself. The team should look at critical components, response, access control, and the perimeter. There are two types of information that is being sought: physical information about the site (layout, distances, capabilities, etc.; and any weaknesses and vulnerabilities that could be exploited by an attacker. It is these weaknesses and vulnerabilities that will be crucial to the development of scenarios later in the process.

Physical Protection System Functions

PPS functions include detect, assess, delay, and respond. Examples of *detection* include; Intrusion Detection Systems (IDS), infrared motion sensors, cameras, and vibration sensors. These detectors are used to notify security personnel of a potential threat and then be able to provide an accurate *assessment*. *Delay* is any barrier that the adversary must get through to advance to the next layer or target, which is calculated as the amount of time it takes to get past each delay element (i.e., doors, walls, fences, authentication, or for cyber, systems

firewalls). *Response* refers to any action taken to stop the adversary from completing the act. For example, a response might interrupt or neutralize the adversary.

To enable the PPS and any connected digital assets to counter a threat, the PPS should perform the following primary functions:

- **Detection and Assessment:** Identify illicit activity at an early stage, which involves prompt detection and accurate assessment
- **Delay:** Impede an attempt to gain unauthorized access, theft, or sabotage by extending an adversary's task time
- **Respond:** Interrupt or neutralize before the adversary can complete his or her task by providing a timely, aware, equipped, and trained response

Please note that while 'deter' is often listed elsewhere as a function of a PPS, there is no adequate way to measure it, therefore, it is not included in the VISA process. Viewed another way, once an attack has commenced it can be assumed that deterrence failed. Either way, it has no role in the VISA process.

Figure 2 depicts the three main functions within a PPS. Each part can be further broken down into people, procedures, and equipment—an important feature when considering potential upgrades to the PPS.

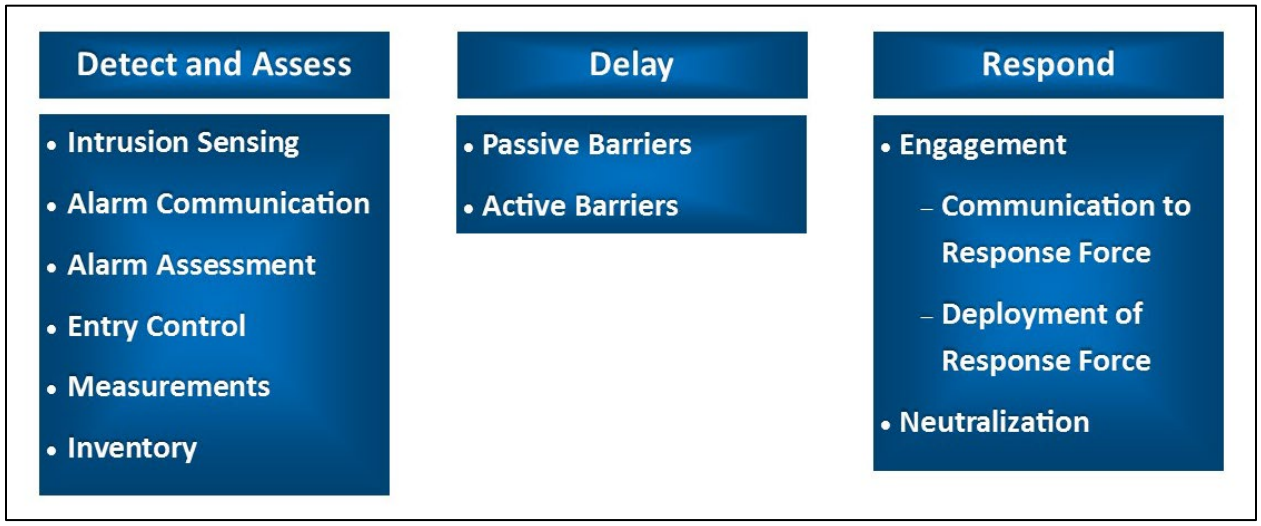

Figure 2: Components of the PPS

Chapter 3: DBT Application & VISA Process Overview

This Chapter provides an understanding of the VISA process and how the DBT is applied throughout this process. It will provide an understanding of what to consider when developing unacceptable consequences, including examples specifically tailored to the industry. This chapter will also highlight the criticality of the response force timeline, including the requirements that are critical to the development of those examples. Next, it will provide a baseline for what factors should be considered during scenario development. Once these baseline fundamentals are addressed, they can then be applied within the VISA worksheet (table examples) which will be highlighted in more detail within Chapter 5.

The VISA Process Overview

Once the SEA team has been finalized and the site characterization details determined, the general VISA process broken down into chronological steps is provided below. The first four fundamental steps will be provided within this chapter. However, detailed examples of steps 4 through 13 are provided within Chapter 5.

1. Develop or refer to the **Unacceptable Consequences** for the site.
2. Determine the **Asset Protection Level** outlined in the DBT and apply it to the site.
3. Develop the **Response Force Timeline**.
4. Develop and **Validate the Scenario**.
5. Divide the scenario into logical steps and provide accurate times for each step.
6. Base Case: analyze system effectiveness for each step.
7. Document any assumptions, notes, and potential upgrades to be considered.
8. Record the overall system effectiveness (OSE) for the scenario.
9. Document the step scores in a tabular format.
10. Assess risk acceptance versus overall system effectiveness.
11. Determine upgrades to be used in the upgrade case.
12. Upgrade case: analyze the same scenario with the upgrades in place.
13. Record the OSE for the upgrade scenario.
14. Run additional upgrade cases as necessary until the threat is mitigated.

Determining Unacceptable Consequences

The first step in the VISA process is to develop unacceptable consequences[3] specific to your site, organization, and/or asset that you need to protect from a given threat within the DBT. The term *unacceptable consequences* refer to a threshold, or consequence, that an owner/operator decides is so severe as to justify expending resources to prevent its occurrence. These can vary among many categories, including reputation, financial, material, or technical, and can go into specifics of losses of particular components, capabilities, or anything that is considered critical to the owner/operator. Additionally, different asset categories (transmission, distribution, and controls) have varying unacceptable consequences with regard to contributing to instability, uncontrolled separation, or cascading failure within an interconnection. For more details please reference, *Chapter 3 of the E-ISAC DBT.*

[3] *Unacceptable consequences* are also related to the asset protection level. High Threat APLs have the most severe consequences. The unacceptable consequence for a low threat APL may simply be the theft of copper grounding straps and cables.

Asset Protection Level and Threat

The next step in the VISA process is for the SEA to apply the appropriate Asset Protection Level and Threat. For example, APL 1 sites would require application of the DBT high-threat information, while APL 3 targets or sites would require the DBT low-threat information. Once the team has categorized the asset as APL 1–3, the VISA process will then demonstrate whether the existing PPS and response can mitigate the threat posed by that DBT level, or if the asset requires added protections. The VISA process can assist the team in determining if upgrades to detect, assess, delay, or response functions are required to sufficiently mitigate the threat. DBT documents can be written at the national or sector level, enterprise level, or the site level.

Note that the SEA team must only use the level of threat that applies to the corresponding APL. Once the team designates the level of the threat, the SEA team must stay within that threat.

A key concept that must be taken into consideration is the SEA team can only use the capabilities outlined within that specific DBT threat level, nothing more. However, the SEA team can use less if it believes it can accomplish the adversary's mission with less. For example, suppose the threat says, "up to three adversaries and 25 lb. of explosives," and the SEA team can accomplish the adversary mission with just one adversary and three lb. of explosives. In that case, the team is staying within the DBT threat level.

Response Force Timeline

The Response Force Timelines (RFT) must be as accurate as possible for the tool to give a credible analysis. For awareness, the RFT should always indicate both an emergency and non-emergency timeline. The **emergency timeline** should represent the amount of time it would take for responders to arrive to the site with the assumption that they know the site is critical. The **non-emergency timeline** should be a *current* and realistic representation indicating the amount of time it would take for responders to get to the site (without knowing the criticality of the site). The steps and times should be as accurate as possible to ensure the analysis is effective. For additional insight, the RFT and adversary timelines are normally determined through performance testing (see **Chapter 6: Performance Testing**). Examples of the RFT are provided below.

Table 5.1: RFT Example (Emergency Run)

Step	Activity	Time (seconds)
1	Alarm annunciation and assessment	45
2	Communication/dispatch to response force (RF)	60
3	RF orients, briefs, begin to move	180
4	RF moves to site (5 min)	600
5	**Armed Response:** Police (2 officers) arrive at 885 and deploy. Set perimeter containment + additional 180. Equipment includes; radios, one patrol rifle, cuffs, flashlights, pistol, body armor, vehicle and handheld radio.	180
Total Response Time		**1065**

Table 5.2 RFT Example (Non-Emergency Run)

Step	Activity	Time (seconds)
1	Alarm annunciation and assessment	45
2	Communication/dispatch to response force (RF)	60
3	RF orients, briefs, begin to move	180
4	RF moves to site (5 min)	600
5	**Armed Response:** Police (2 officers) arrives at 10 min after the primary response (885) + 600 for transit, + 80s to deploy = same equipment as primary response.	680
Total Response Time		**1565**

Task Time versus Response Time

The SEA team needs to have an understanding of the response time, while also taking into consideration the task time of the adversary pathway. Another consideration that should be applied is at what points the PPS is going to be able to accurately detect and assess the adversary to initiate the response force timeline so the responders engage the adversary.

Figure 3.1 provides an example of a very high probability of engagement.

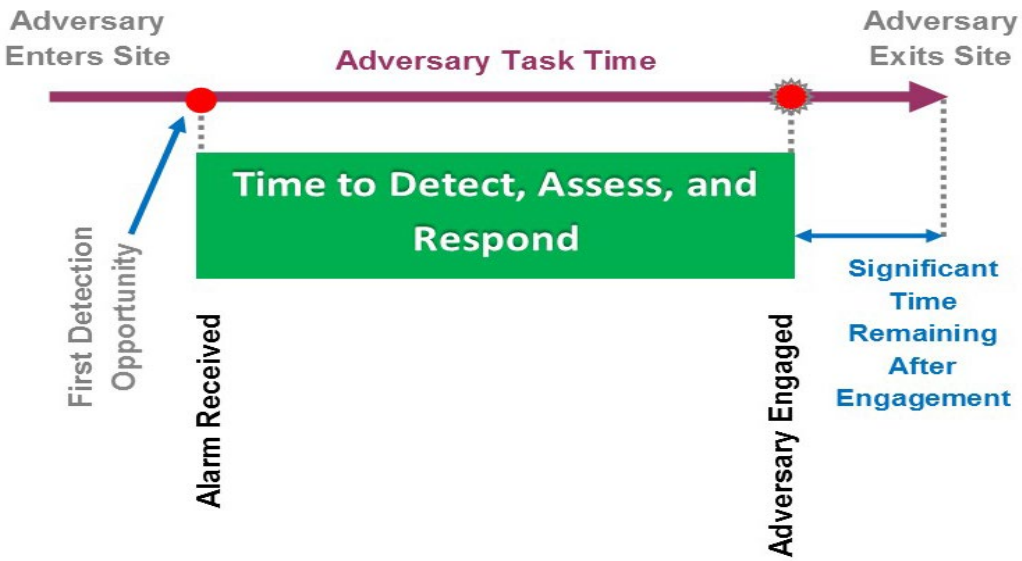

Figure 3.1: Sample Task Time versus Response Time

Figure 3.2 provides an example of a very low probability of engagement. The PPS is not able to detect, delay, and effectively respond to a specified threat.

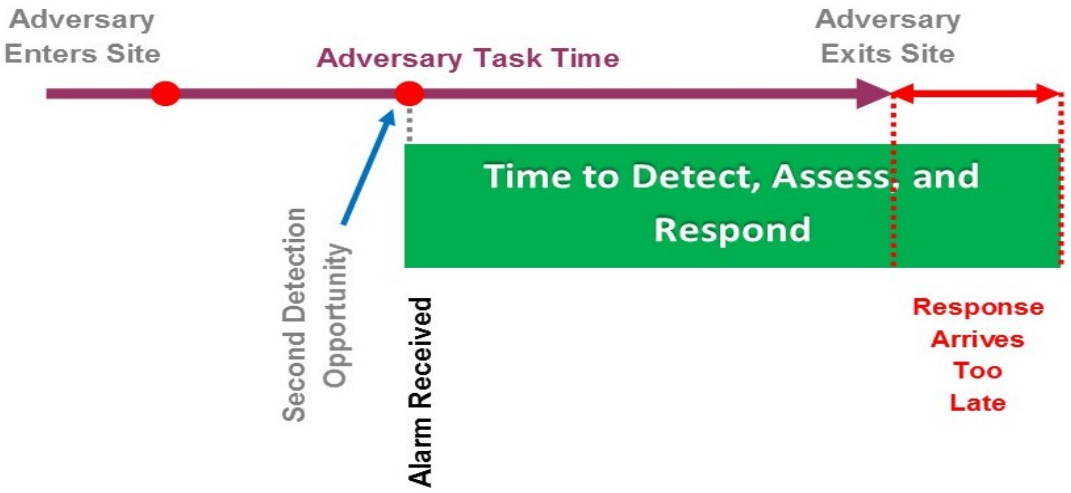

Figure 3.2: Sample of Late Response Time

Scenario Development Methodology

When developing a scenario, the SEA team will exploit potential weaknesses in the PPS and connected components by using a credible and realistic plan that gives the adversary the best chance for success. As previously noted, it's critical to use only the parameters that are included within the DBT and nothing more, but it could be less. Once the SEA team has a concept in mind, they will develop a credible and realistic scenario and break the scenario down into logical steps with corresponding times for each step (see examples in Chapter 5).

Every scenario should stand up to the "reasonable and credible" test. The adversary's goal is usually intended to exploit a weakness in the PPS, including personnel, procedures, and equipment. The scenario is discussed, agreed to, and then documented by the SEA team for every analysis run. The SEA team may want the adversary to use a specific pathway to the target or a particular tactic such as "stealth until discovered." The same adversary run must also be used for the upgrade case to see if the proposed PPS upgrades and response are effective[4].

There are three different types of scenarios that will incorporate different adversaries. The first example in Chapter 5, will highlight an outsider case scenario, followed by an insider case scenario, and finally, a scenario involving outsider(s) colluding with and insider. Before developing the scenarios, it's important to follow the parameters set within the DBT which serve as a critical resource to ensure that each scenario is reasonable and credible.

Outlined in *Chapter 1 of the Electricity Sector DBT* are definitions for what constitutes an "outsider" and an "insider".

- **Outsider** refers to a person who does not have unescorted access to a facility. An outsider may have the intent to engage in theft, damage, or destruction of critical equipment or infrastructure with or without general industry knowledge. Other actions to be considered are kidnapping, threats and/or violence against personnel, a standoff attack against a facility, and cyber-enabled attacks.

- **Insider** refers to a current or former employee, contractor, or business partner who has or has had authorized access to an organization's network, system, data, or facilities. An insider may circumvent or abuse authorized access in a manner that negatively affects the confidentiality, integrity, or availability of an organization's information or its information systems, the operation of the BPS, the safety of employees, or the security of assets. Insiders are often privy to information that would be difficult or impossible for an outsider to obtain. This can include custom implementations of security or operating systems, idiosyncrasies in personnel or procedures, pattern-of-life information, equipment malfunctions, or other uncorrected vulnerabilities.

  An insider may circumvent or use access in a manner that negatively affects the confidentiality, integrity, or availability of an organization's information or information systems, the operation of the BPS, the safety of employees, or the security of assets.

  - **Passive Insider:** A passive insider may pass information to an outside adversary group to assist in accomplishing its goal, whether through malicious intent or unintentionally. This information can come in the form of intellectual property, blueprints, operational knowledge, documents,

[4] *Occam's Razor states the simplest explanation is preferable to one that is more complex. Scenarios serve to solve problems: how can I achieve this unacceptable consequence given these resources and this PPS? Adversaries can reasonably be expected to use the simplest plan that would give them a reasonable chance of achieving their aim, as these have fewer dependent actions and less resources. The aim of the scenario is to test the PPS, not create a novel. Keep scenarios simple.*

security procedures, and physical protection system knowledge. The passive insider does not participate in any other way.

- **Active Nonviolent Insider:** An active nonviolent insider can act either alone or together with outside adversaries. This insider can provide information like the passive insider and also use authorized access and authority, in addition to stealth and deceit. Active nonviolent insiders may also conduct disruptive actions, such as IT sabotage (e.g. manipulating security networks and other control systems), insider fraud and/or espionage. Nonviolent disruptive actions may also include limited physical damage (such as damaging computer equipment or cutting fiber optic cables).
- **Active Violent Insider:** The active violent insider will use their specialized knowledge and skillset to penetrate and maximize physical damage against an organization's security, systems, and critical assets. They are willing to risk death and/or use deadly force, and possibly weapons, against personnel or critical components in an attempt to complete their mission.

Using only what is listed within the applicable DBT threat level, the development of a scenario should consider the following:

- Develop an adversary force organization. This organization identifies the numbers, roles, responsibilities, and skill levels of each adversary in the group.
- Identify equipment and weapons that each adversary will be carrying (be specific).
- Identify tactics, pathways, techniques, and procedures (e.g., abrupt, violent theft, criminal mischief, covert tactical entry, and surprise, speed, and violence of action).
- Consider pre-attack activities (e.g., social engineering, penetration testing, diversions, or supplemental activities).
- Develop a general concept of operation. This is the scenario to be assessed.
- Break the scenario down into logical steps and task times and add as much detail as possible to each step.
- Develop a realistic and credible timeline for each step that can be analyzed.
- Complete the outsider scenario table (discussed in the Scenario and Response Tables section)

Chapter 4: Evaluation

This chapter is intended to provide an understanding of how to evaluate each step and activity through the use of the VISA tool and methodology.

Evaluation of the Steps

Each step and associated action represent a potential opportunity to detect, assess, engage, and neutralize the adversary. The SEA team must look at each step individually and determine whether the PPS can meet these opportunities within those parameters. The VISA methodology can be either quantitative or qualitative. The quantitative approach involves numerical calculations of system effectiveness based on specific values for probabilities of detection, assessment, engagement, and neutralization. The qualitative approach is more intuitive in that through the process of analysis, ratings are assigned to the probabilities of detection, assessment, engagement, and neutralization rather than specific numbers, and the overall system effectiveness is derived from a logical process. While more accurate, the quantitative method can be somewhat cumbersome to calculate by hand for each scenario. The qualitative method, while less accurate, is less time-consuming and provides a more general estimate of system effectiveness. The SEA team normally uses the qualitative method and evaluates each of the following steps as if the proceeding step had been successful.

Detection

During detection, security personnel are drawn to automated alerts, security sensors, local alarms, and observation. For example, if an adversary walks into the center of a detection zone where a sensor is located, the probability of detection would be very high. If the adversary only skirts around the edge of the detection zone, then the SEA team must discuss and agree on a moderate step score. SMEs can determine the likelihood of sensor effectiveness on the outside fringe of a detection zone. While one sensor might have a high detection probability in the center of its coverage, the area on the edge might be very low. This also demonstrates the need for overlapping and complementary sensor types to eliminate a single point of weakness or failure.

Accurate Assessment

Accurate assessment can occur only once a threat is detected. Accurate assessment involves initiating a security response after correctly determining that the detected action poses a threat to the overall system effectiveness. Assessment capabilities could include cameras, guards, site personnel, and established procedures. A perimeter sensor may alarm and give the PPS credit for detection, however, unless you can observe and assess what initiated the alarm, you cannot have a high probability of accurate assessment. Assessment values can be determined from published data, performance testing, and SME judgment. Accurate assessment should give you the ability to determine the following:

1) Whether the detection is a false, nuisance, or valid alarm
2) Determine where or when the detection occurred, and what caused the alarm.

Engagement

Engagement can occur only once a threat is detected and accurately assessed. Engagement is the ability of a security response force to arrive, deploy, and engage an adversary. Engagement is typically time-dependent and should be as accurate as possible. The most effective way to gather accurate response times is to conduct performance testing. This can be accomplished by using the PPS or supporting critical digital assets to initiate alarms and gather data on the time it takes for responders to arrive and deploy in a manner that is capable of interrupting the adversary (see **Chapter 6: Performance Testing**). Initially, the SEA will make their evaluations for the probability of engagement based on the response force timelines.

Assessment of engagement will require an understanding of the response force's tactics, techniques, and procedures. You cannot assume the arrival of one police officer qualifies as engagement, as police procedures may require them to observe from a safe location and call for backup. In this case, engagement may begin with the arrival of the backup force. This is why it is critical to have a local law enforcement representative(s) join the SEA team.

Neutralization

Neutralization can occur only once a threat is detected, accurately assessed, and engaged. Neutralization is the ability of the organization's response plans and procedures to prevent the adversary from completing the mission. Effective neutralization requires superior knowledge, skills, numbers, and capabilities of the response force. The probability of neutralization is based primarily on the techniques, tactics, and procedures of the response force and their abilities to stop the adversary at a specific point in the timeline. Additional classifiers taken into consideration are training, weapons, equipment, and motivation of each side. For example, if six heavily-armed and highly-trained responders contain a single adversary with a pistol in a small space, the probability of neutralization would be high or very high for the responders.

Step Scores are Independent

Focus the discussion and evaluation only on the specific step the SEA team is addressing. If at any time, a step in the scenario has achieved sufficient detection and assessment to stop an adversary (and, for the outsider, enough time remaining for engagement and neutralization) the PPS was successful enough to stop the attack.

Explanation of the Evaluation

The step scores indicate the weakest point of that layer (see Chapter 5, **Table 5.3**). One cannot expect the PPS and its connected systems to perform better than its weakest point. The overall system effectiveness score (shown in red) is the highest of all the step scores. This is where one takes credit for the best-performing part of the PPS. It is driven by the weakest point for the adversary and the strongest point for the PPS. In the example listed in **Table 5.3,** step 12, the PPS can take credit for detection and assessment, but the responders never make it to the site in time to have any effect on the adversaries. The adversaries have already completed the act and have departed the site by the time the response arrives on site.

Chapter 5: Scenarios

This chapter provides three different scenarios, as well as examples of how the VISA tool and methodology are implemented. Based on the information highlighted in the previous chapters, participants should have a fundamental baseline understanding of how to develop credible scenarios, and accurate timelines, as well as how to effectively evaluate each step of the scenario utilizing the tool and methodology. This chapter will provide different scenario examples, including a base case and an upgrade case for each, including examples of how each step is evaluated. The first example highlights an outsider's adversary plan; the second example provides an insider's adversary plan; and the third and final example involves outsider(s) colluding with insider(s) adversary plan. Throughout each example, it is *essential* to capture all assumptions made, detailed notes, as well as potential upgrades discussed within the applicable table(s).

Outsider Example:

Outsider Adversary Plan

Provided below is an example of an adversary plan involving an outside attack scenario on transformers using the high threat from the DBT:

Scenario: At 0200 on 5 July three outsiders approach the southeast (SE) perimeter wall in a van without lights at 0200, and park 25 m from the wall. Outsiders 2 and 3 unload a ladder and backpacks and move tactically to the perimeter wall. Outsider 1 remains with the vehicle. Outsiders 2 and 3 stealthily bridge over the wall using the ladder and then move to the first transformer. The ladder is left in place. Outsider 2 provides security for outsider 3 while he sets and primes the first explosively formed projectile (EFP) charge 1 meter from the eastern transformer and sets the detonating time for 0215. Outsiders 2 and 3 move to the western transformer and repeat the process for the second EFP charge. Outsiders 2 and 3 run back to the wall, go over the wall together, and exit the site. They then move back to the vehicle and depart the area. At 0215, both EFPs detonate.

This is a good time for the SEA team to step back and re-check if this is a valid scenario. It is valid if it meets the following criteria: 1) reasonable and credible; 2) stays within the DBT; 3) achieves one or more unacceptable consequences. The following are examples of site-level unacceptable consequences:

- Loss of one or more of the transformers for six months or more
- Loss of the ability to control the substation from the control room for one month or more
- Unauthorized access and malicious manipulation or destruction of the control room, switching racks, or battery banks
- Loss of life or serious injury on the substation property
- Unauthorized use of badge credentialing software

Outsider weapons, ammunition, equipment, and other supplies should be noted on a separate document for each scenario. Remember, each step represents a potential opportunity for the PPS and response systems to detect, assess, engage, and neutralize the adversary. Once the scenario has been validated, participants should break it down into steps, and assign times for each action (**Table 5.3**).

Response Force Timeline

As noted in Chapter 3, the RFT must be as accurate as possible for the tool to give a credible analysis. As a reminder, the RFT should indicate an emergency and non-emergency response timeline. The **emergency timeline** should assume that First Responders (LEO/Fire) prioritize the impacted site and respond with lights and sirens when breaking out the step activity and times (**Table 5.1)**. The **non-emergency timeline (Table 5.2**) should represent the timeline it would take to respond at normal traffic speeds. Response Force Times and Adversary Timelines are normally determined through performance testing (see **Chapter 6: Performance Testing**).

Table 5.1: RFT Example (Emergency Run)		
Step	**Activity**	**Time (seconds)**
1	Alarm annunciation and assessment	45
2	Communication/dispatch to response force (RF)	60
3	RF orients, briefs, begin to move	180
4	RF moves to site (5 min)	600
5	**Armed Response:** Police (2 officers) arrive at 885 and deploy. Set perimeter containment + additional 180. Equipment includes; radios, one patrol rifle, cuffs, flashlights, pistol, body armor, vehicle and handheld radio.	180
Total Response Time		**1065**

Table 5.2 RFT Example (Non-Emergency Run)		
Step	**Activity**	**Time (seconds)**
1	Alarm annunciation and assessment	45
2	Communication/dispatch to response force (RF)	60
3	RF orients, briefs, begin to move	180
4	RF moves to site (5 min)	600
5	**Armed Response:** Police (2 officers) arrives at 10 min after the primary response (885) + 600 for transit, + 80s to deploy = same equipment as primary response.	680
Total Response Time		**1565**

The total RFT of the **emergency** timeline example is **1065** seconds (Table 5.1), and 1565 seconds for the **non-Emergency** (Table 5.2).

Outsider Scenario Base Case Example

In Table 5.3 below, three columns track time (in seconds). These include the **Step Time** for the adversary's actions, the **Cumulative Time** of the adversary's actions, and the **Response Force Timeline** for the responders. The **Cumulative Time** for the outsider scenario is 810 seconds, as noted in Step 12, which is less than the response force timeline. Therefore, law enforcement would not arrive in time before the adversary detonates the explosives. After completing the steps and timelines, it is time to complete each of the evaluation steps (P_D (detection), P_A (assessment), P_E (engagement), and P_N (neutralizing)). Chapter 4 serves as a helpful reference guide when conducting the evaluation.

Table 5.3: Outsider Scenario Base Case Example									
Step	**Step Time (seconds)**	**Cumulative Time (seconds)**	**Remaining Response Force Time**	**Step Description**	**P_D**	**P_A**	**P_E**	**P_N**	**Step Score**
1	-	-	-	At 0200 on 5 July three adversaries (outsiders) arrive at in a blacked-out vehicle and park 25 m away from the SE perimeter wall.	VL	VL	VL	VL	**VL**
2	120	120	-	Outsider 1 remains with the vehicle. Outsiders 2 and 3 quietly unload a ladder, and prepare 2-kg EFPs, weapons, battery-powered tools, and a small backpack each.	VL	VL	VL	VL	**VL**

Table 5.3: Outsider Scenario Base Case Example									
Step	**Step Time (seconds)**	**Cumulative Time (seconds)**	**Remaining Response Force Time**	**Step Description**	**P_D**	**P_A**	**P_E**	**P_N**	**Step Score**
3	45	165	-	Outsiders 2 and 3 stealthily approach the SE perimeter wall at 0200 carrying a ladder, rifles, pistols, radios, 2 EFPs, small backpacks, and night vision goggles (NVG). The ladder is left in place (same exit point).	VL	VL	VL	VL	**VL**
4	90	255	-	Outsiders 2 and 3 use the ladder to quietly bridge over the wall.	L	L	VL	VL	**VL**
5	45	300	-	Outsiders 2 and 3 tactically move 75 m to the eastern transformer with the weapons, backpacks, and two EFPs.	L	L	VL	VL	**VL**
6	90	390	-	Outsider 2 provides security as outsider 3 places, primes, and sets the detonating time of 0215 on the first EFP.	L	L	VL	VL	**VL**
7	20	410	-	Outsiders 2 and 3 tactically move 50 m to the western transformer.	L	L	VL	VL	**VL**
8	90	500	-	Outsiders 2 and 3 repeat step six.	L	L	VL	VL	**VL**
9	25	525	-	Outsiders 2 and 3 run back 125 m to the wall.	L	L	VL	VL	**VL**
10	45	570	-	Outsiders 2 and 3 quickly move back over the wall and run back to the van.	L	L	VL	VL	**VL**
11	30	600	-	All outsiders drive normally to the main road and depart the area; 3.5 min (210s) remaining on the EFP timers.	VL	VL	VL	VL	**VL**
12	210	**810**	**1065**	At 0215, both EFPs detonate.	VH	M	VL	VL	**VL**
				Overall System Effectiveness:					**VL**
Legend: Probability of: Pd = Detection; Pa = Assessment; Pe = Engagement; Pn = Neutralization									
Legend: VL = Very Low; L = Low; M = Medium; H = High; VH = Very High									
Legend: Times are in seconds (s)									

Once the evaluation has been completed and all assumptions and notes have been documented in Table 5.3., the next step is to determine potential upgrades that could be implemented to cause a delay or prevent the adversary from carrying out their plan. List all upgrades under the applicable section of Table 5.3 (see below) and put an asterisk next to the upgrades the SEA team determines to be adequate. Reference the next section that highlights *Determining Potential Upgrades for the Outsider Scenario*.

Table 5.3: Outsider Scenario Base Case Assumptions and Upgrade Notes
Assumptions
Step 1: The outsider vehicle is not observed by PPS arriving next to the SE perimeter.
Step 6: At the end of this step, the local time will be 1411 hours and 30 seconds.
Step 4-10: Some credit is given for Detection and Assessment (D&A) due to casual observation of a switchyard worker at that time. No part of the current PPS can achieve any D&A for those steps.

Step 12: Onsite personnel will hear the explosions (Detection). However, no assessment capabilities are looking at the transformers. Onsite workers will observe post-blast destruction including smoke and fire.
Step 12: Someone onsite will call 911 and report explosions and fire at the substation, however, will not report an attack on the substation. Fire will respond to the site; however, police may not respond until the ladder left behind by the adversaries is noticed at the perimeter wall.
All System Changes or Upgrades considered (used in upgrade scenario)**
****** **1) Delay // 8-foot anti-cut, anti-climb metal mesh fence installed around both transformers – 9 minutes delay with power tools (36V battery powered reciprocating saw); performance test it before install.**
****** **2) Program – Procedure // Establish a performance testing program for D&A on the perimeter.**
****** **3) D&A // Install video motion detector (VMD) and lighting and razor wire on the perimeter wall.**
4) **Response** // Onsite armed guard force – three people per shift w/ pistols, flashlights, cuffs, pepper spray. Trained and performance tested. Detain and deadly force authority/policy written, and knowledge tested.
5) **Response** // Exterior perimeter random patrols by local law enforcement.
****** **6) Response // Host a site visit with local law enforcement to inform and raise the priority of the dispatch call to the site. Response time reduced from 1065s to 945s.**
7) **Detect** // Install buried vibration detection system (1-m exterior to the perimeter wall).
****** **8) D&A // Install a backup alarm notification system at the district grid control center - off-site.**
9) **Assessment** // Install two pole-mounted close-captioned televisions with VMD in the switchyard - each looking at the transformers.
Notes
Scenario: Response is never started until the explosives go off on step 12.
Idea: Pole-mounted VMD and lighting on the SE perimeter wall - min 2-m coverage on both sides.
Need D&A on the perimeter
Need more delay on this pathway to the transformer

Determining Potential Upgrades for the Outsider Scenario

The SEA will determine where the PPS and the response force require improvement to mitigate the threat. They will consider people, procedures, and equipment for each PPS function (detection, accurate assessment, engagement, and neutralization). It's important to note that the SEA team is not concerned with the cost of upgrades; their job is to determine how to mitigate the threat. After the SEA is complete, the risk managers will have the ability to make informed risk-based decisions on where to apply funding for the upgrades, and whether or not they are going to accept the risks.

Once the potential upgrades have been determined, the SEA team will re-run the same scenario using the same threat and adversary plan; however, this time the team will now apply the potential upgrades to each applicable step and note the increased Overall System Effectiveness (OSE), referred to as the "upgrade case." It may take several upgrade scenarios to determine what risk is acceptable, versus the cost of the proposed upgrades and/or improved response. Each upgrade case will be documented. As a general practice, upgrades that were considered, but not used, should still be captured and documented for potential future use in other scenarios. General PPS improvements that are typically considered are as follows:

- **Increased Detection:** Increasing the capability of earlier detection using overlapping complementary sensors. This allows for accurate assessment meaning the response timeline can start earlier.
- **Improved Assessment:** Consider Providing additional camera or security personnel coverage. Detection cannot happen without accurate assessment.
- **Longer Delay:** The greater the delay or the more barriers the adversaries must negotiate, yields more time for responders to arrive.
- **Quicker Response Force Times:** Move responders closer to the asset/site to be effective or have responder's onsite full time.

- **More Effective Neutralization:** Ensure the responder-to-adversary ratio is adequate. For example, the responders have added site and system knowledge, improved skills, better weaponry, training, and equipment, and are directed to the best response positions to achieve their goal.

Table 5.4 Outsider Scenario Upgrade Case Example

Step	Step Time (seconds)	Cumulative Time (seconds)	Remaining Response Force Time	Step Description	P_D	P_A	P_E	P_N	Step Score
1	-	-	-	At 0200 on 5 July three adversaries (outsiders) arrive at in a blacked-out vehicle and park 25 m away from the SE perimeter wall.	VL	VL	VL	VL	**VL**
2	120	120	-	Outsider 1 remains with the vehicle. Outsiders 2 and 3 quietly unload a ladder, two prepared 2-kg EFPs, weapons, battery-powered tools, and a small backpack each.	VL	VL	VL	VL	**VL**
3	45	165	-	Outsiders 2 and 3 stealthily approach the SE perimeter wall at 0200 carrying a ladder, rifles, pistols, radios, 2 EFPs, small backpacks, and night vision goggles (NVG). The ladder is left in place (same exit point). **Upgrade 2, 3**	VL	VL	VL	VL	**VL**
4	90	255	945	Outsiders 2 and 3 use the ladder to quietly bridge over the wall. **Upgrade 2, 6, 8**	VH	VH	VL	VL	**VL**
5	45	300	900	Outsiders 2 and 3 tactically move 75 m to the eastern transformer with the weapons, backpacks and two EFPs.	VL	VL	VL	VL	**VL**
6	690	990	210	Outsider 2 provides security as outsider 3 places, primes, and sets the detonating time of 0215 on the first EFP. **Upgrade 1**	VH	VH	VL	VL	**VL**
7	20	1,010	190	Outsiders 2 and 3 tactically move 50 m to the western transformer.	VL	VL	VL	VL	**VL**
8	690	1,700	Plus 500	Outsiders 2 and 3 repeat step six. **Upgrade 1**	M	M	H	L	**L**
9	25	1,725	Plus 525	Outsiders 2 and 3 run back 125 m to the wall.	M	M	H	L	**L**
10	45	1,770	Plus 570	Outsiders 2 and 3 quickly move back over the wall and run back to the van.	VH	VH	H	L	**L**
11	30	1,805	Plus 605	All outsiders drive normally to the main road and depart the area; 3.5 min (210s) remaining on the EFP timers.	VL	VL	M	L	**VL**
12	210	**2,015**	Plus 815	At 0215, both EFPs detonate.	-	-	-	-	
								Overall System Effectiveness:	**L**
Legend: Probability of: Pd = Detection; Pa = Assessment; Pe = Engagement; Pn = Neutralization									
Legend: VL = Very Low; L = Low; M = Medium; H = High; VH = Very High									

Table 5.4: Outsider Scenario Upgrade Case Assumptions and Upgrade Notes
Assumptions
Step 8: Adversary vehicle will be spotted and adversary 1 will be contacted by 1 police officer.
Step 6: First EFP will detonate near the end of this step - at 0216 hrs. 35s
All System Changes or Upgrades considered (used in the upgrade scenario)**
1) **Delay** // 8-foot anti-cut, anti-climb metal mesh fence installed around both transformers - 10 min // 600s delay with power tools (36-V battery powered reciprocating saw / carbide blade); performance test it before install.
2) **Program - Procedure** // Establish a performance testing program for D&A on the perimeter.
3) **D&A** // Install VMD and lighting and razor wire on the perimeter wall.
8) **D&A** // Install a backup alarm notification system at the district grid control center - off-site.
6) **Response** // Host a site visit with local law enforcement to inform and raise the priority of the dispatch call to the site. Response time reduced from 1065s to 945s.
Notes
Step 8-10: Primary response arrives and deploys to set containment - will not enter an energized site. The probability of neutralization will be moderate (4 armed adversaries vs. 2 police officers)
Scenario Clock vs. Delay Timer: End of step 2 = time is 0202, end of step 3 = time is 0202:45, end of step 4 = time is 0204:25s, end of step 5 = time is 0205:05s, end of step 6 = time is 0216:35s (first EFP detonates).
Step 5: No D&A inside the switch yard - just on the perimeter.
Step 10: Scenario ends. Even though the OSE is L, one transformer is still lost in step 6.
Need more delay before the adversary gets to the first transformer.
Need to look at additional upgrades.

Once the outsider upgrade case has been validated and all documentation is complete, the SEA team will document the upgrades that were identified throughout the outsider scenario. This information can either become part of the upgrade archive repository or it can be presented as viable upgrades to the risk manager(s). This will allow the risk manager(s) to then be able to make an informed risk-based decision for what the utility or organization deems to be essential.

Insider Example:

Insider Considerations for Scenario Development

When developing an insider threat scenario(s), it is critical to utilize only what is listed within the DBT. Listed below are things to consider when developing insider scenarios:

- List tactics, techniques, and procedures (e.g., theft, criminal mischief, covert entry, surprise, cover for action, cover for status, and ignoring alarm annunciations on a display).
- Consider pre-attack activities (e.g., diversions or supplemental activities, leaving a door unlocked or ajar, upgrading badge access, sharing log-on credentials to critical systems, misreporting or not reporting something that could indicate pre-attack preparations).
- Develop a general concept of the operation, including the unacceptable consequence to be achieved. This is the scenario to be assessed.
- Break down the insider base case scenario into logical steps and add as much detail as possible (**Table 5.5**).
- Fill out the insider base case scenario table (**Table 5.5**) and develop a task time for each step.

- Identify a single individual with access to the high-consequence asset who is:
    1. Willing to misuse access and authority or share sensitive information.
    2. Not willing to use violence or force.
    3. Willing to take advantage of known vulnerabilities, lack of procedures, or other weaknesses.

Nonviolent insider scenarios generally only involve detection and assessment and do not include engagement and neutralization because their activities often violate company policy, not criminal law, so the law enforcement would not have jurisdiction

Insider Adversary Plan

Provided below is an example of an adversary plan involving an insider attack scenario that achieves the unacceptable consequence of 'unauthorized access and malicious manipulation or destruction of the control room, switching racks, or battery banks.'

Scenario: A disgruntled IT network engineer working for a utility is dissatisfied with his work environment, due to a lack of advancement following his performance review. Due to his feelings of dissatisfaction, he uses his company card over the weekend to purchase personal items. These actions cause him to become paranoid, therefore, he abuses his level of authorized network access on Tuesday of the following week to monitor for any internal communications and discovers that he is the subject of an internal HR investigation. After his discovery, he becomes angry and plans an attack on one of the utility's substations that is adjacent to a busy building supply store. As a part of his attack preparations, he assembles the following tools; personal laptop, handheld ratchet wire cutters, and his issued master key (this master key provides access to all utility substations and is issued to several utility employees). Next, he conducts a spoofing attack[5] by creating a local VPN admin account using the same name as the HR manager, which then grants him unique capabilities that only the HR manager has authorized access to. Two days following the discovery of the investigation, he proceeded to carry out his attack. At the end of the day on Thursday, he exits the main office building at 1730 and drives to the building supply store parking lot (adjacent to the substation) in his personal vehicle to provide concealment and cover near the loading area. He brings with him his personal laptop, handheld ratchet wire cutters, and issued master key. While in the vehicle, he opens his laptop and connects to his personal cell phone hotspot, and logs into the VPN to access the corporate network using the HR director's spoofed account. Once in the network he accesses the substation's access control system and disables it, preventing any detection via cameras. He exits his vehicle and walks 50 yards to the west vehicle gate of the substation (adjacent to the building supply parking lot). Using his issued master key, he unlocks the padlock on the vehicle gate, places the padlock into his pocket, and enters through the gate, closing the gate behind him. He then walks 25 yards from the gate to the control house building, uses his master key to unlock the deadbolt, swipes his badge at the access control panel, and opens the door. Once inside, he opens all breaker handles and proceeds to cut the main cable coming down the side of the panel with the handheld wire cutters, which results in total loss of control of the substation. He walks out of the control house (leaving the door open behind him), proceeds to the building supply store vehicle gate, walks to his personal vehicle, and leaves the site.

Insider Base Case Example:

In **Table 5.5** below, two columns track time. These include the **Step Time** for the adversary's actions and the **Cumulative Time** for the adversaries. As noted above, nonviolent insider scenarios generally only involve detection and assessment and do not include engagement and neutralization, therefore, the **Response Force Timeline** does not apply in this example. The **Cumulative Time** for the insider scenario is 1,165 seconds. After completing the steps and step timelines, it is time to complete the evaluation of each step (detection,

[5] Spoofing, as it pertains to cybersecurity, is when someone or something pretends to be something else in an attempt to gain our confidence, get access to our systems, steal data, steal money, or spread malware.

assessment, and overall step score). Step 10 highlighted in yellow represents where the PPS must stop the adversary in order to successfully prevent the attack from achieving the unacceptable consequences.

Table 5.5: Insider Scenario Base Case Example

Step	Step Time (secs)	Cumulative Time (secs)	Remaining Response Force Time	Step Description	P_D	P_A	P_E	P_N	Step Score
1	-	-		A disgruntled IT network engineer working for a utility is dissatisfied with his work environment, due to lack of advancement following his performance review. Due to his feelings of dissatisfaction, he uses his company card over the weekend to purchase personal items.	M	VL			**VL**
2	-	-		These actions cause him to become paranoid, therefore, he abuses his level of authorized network access on Tuesday of the following week to monitor for any internal communications and discovers that he is the subject of an internal HR investigation. After his discovery, he becomes angry and plans an attack on one of the utility's substations that is adjacent to a busy building supply store. As a part of his attack preparations, he assembles the following tools; personal laptop, handheld ratchet wire cutters, and his issued master key (this master key provides access to all utility substations and is issued to several utility employees).	VL	VL			**VL**
3	180	180		Next, he conducts a spoofing attack by creating a local VPN admin account using the same name as the HR manager, which then grants him unique capabilities that only the HR manager has authorized access to. Two days following the discovery of the investigation he proceeds to carry out his attack.	H	VL			**VL**
4	360	540		At the end of the day on Thursday, he exits the main office building at 1730 and drives to the building supply store parking lot (adjacent to the substation) in his personal vehicle to provide concealment and cover near the loading area. He brings with him his personal laptop, handheld ratchet wire cutters and issued master key.	VL	VL			**VL**
5	120	660		While in the vehicle, he opens his laptop and connects to his personal cell phone hotspot, and logs into the VPN to access the corporate network using the HR director's spoofed account.	VH	VL			**VL**

6	120	780		Once in the network he accesses the substation's access control system and disables it, preventing any detection via cameras.	H	VL			**VL**
7	60	840		He exits his vehicle and walks 50 yards to the west vehicle gate of the substation (adjacent to the building supply parking lot).	VL	VL			**VL**
8	10	850		Using his issued master key, he unlocks the padlock on the vehicle gate, places the padlock into his pocket, and enters through the gate, closing the gate behind him.	VL	VL			**VL**
9	30	880		He walks 25 yards from the gate to the control house building, then uses his key to unlock the deadbolt, swipes his badge at the access panel, and opens the door.	H	VL			**VL**
10	210	1,090		Once inside, he opens all breaker handles and proceeds to cut the main cable coming down the side of the panel with the handheld wire cutters, which results in total loss of control of the substation.	VL	VL			**VL**
11	75	**1,165**		He walks out of the control house (leaving the door open behind him), proceeds to the building supply store vehicle gate, walks to his personal vehicle, and leaves the site.	VL	VL			**VL**
								Overall System Effectiveness:	**VL**
Legend: Probability of: Pd = Detection; Pa = Assessment; Pe = Engagement; Pn = Neutralization									
Legend: VL = Very Low; L = Low; M = Medium; H = High; VH = Very High									

Table 5.5: Insider Scenario Base Case Assumptions and Notes
Assumptions
Step 1: The insider has not displayed significant indicators of dissatisfaction, leading to difficulty in detection/assessment during this step.
Step 6: Following the loss of the switch, the insider along with four others will receive alerts (with a lag of ~15 minutes), however once alerted, the other personnel will likely assume that the insider will be called to investigate.
Step 10 is where we have to stop the insider from completing the act.
All System Changes or Upgrades considered (used in the upgrade scenario)**
**** 1. Program-Procedure // Insider threat awareness training included with annual security refresher training (all staff). (step 1)**
2. Crisis intervention team / Insider threat risk management team (ITRM team); the team is assembled to develop a plan of action or way forward. The ITRM team is comprised of an individual's manager, director, HR, legal, security representative, IT/cybersecurity representative, and any required third-party support groups or individuals.
**** 3. D&A // Software that can recognize when an individual is accessing email inappropriately.**
4. Oversight and monitoring system including administrative access logs, and monthly reviews to recognize unusual access and require post-validation of access.
5. Employee well-being sustainment program
6. Procedures for reducing access during an investigation - must happen after critical conversations with the employee being investigated, including notification of investigation. Known suspects vs. unknown suspects require different procedures.
7. Establishing background check and re-check processes including identification of positions of high trust.
**** 8. D&A // Add alerting to administrative/configuration changes to VPN.**
9. Additional validation to require pre-authorized systems for VPN access.
**** 10. D&A // Develop security-only network: Segregating IDS and VSS from corporate network and SCADA network.**
**** 11. D&A // Cyber key with a master key capability that requires secondary approval for access.**
12. Extend monitored access controls to both vehicle gates.
13. Frequent vs. infrequent use notifications (security culture may require adjustments).
**** 14. D&A // Temporary access release through Dispatch - i.e., personnel visiting the control house would be required to call Dispatch to request access with remote access granted by Dispatch only, which requires additional technical solutions to address loss-of-power and loss of communications scenarios. Could also include a work authorization system, including software, policy, and procedure. Could be restricted to after-hours work only, or when one person is working alone.**
**** 15. D&A // Two-Person Rule (TPR) is in effect for all network engineers working inside a control building. The second person must be in a similar job position and must maintain line-of-sight of the work being done while inside the control house.**
Notes
Step 1: 1. Consider developing annual security awareness training to include insider threat awareness for all staff.
Step 6: Even though Dispatch has visibility with cameras, it will not raise any alarm during this step since connectivity issues can often lead to loss of signal. 2. Consider developing a loss of communications plan for escalation time frames and processes for alerting. 3. Existing equipment has alerting capability for loss-of-node but is not currently in use. 4. No formal response procedure exists for losing a switch. 5. There are methods to work around loss-of-switch alarming--by disabling the intrusion detection system and camera ports directly rather than disabling the switch.
Step 9: The badge reader will store information about badge activity locally only, which will be downloaded once communications are re-established.
Step 10: During this step, operations will receive multiple device open alarms. Operations dispatch is now aware of highly abnormal operations at the substation.

Determining Potential Upgrades for the Insider Scenario

After the SEA team validates the insider example, it is time to identify potential upgrades and run one upgrade case to support the insider scenario (see **Table 5.6**). Using the insider base case scenario and applying the upgrades to the applicable steps, it raised the OSE to "Very High" which is highlighted below in **Table 5.6** in **Green**. This indicates the potential upgrades have stopped the insider before they can complete the act. If the OSE is not at an acceptable level, several upgrade runs may be required, or where the risk is determined to be acceptable by the security and/or risk manager (not the SEA team).

Table 5.6: Insider Scenario Upgrade Case Example

Step	Step Time	Cumulative Time	Remaining Response Force Time	Step Description	P_D	P_A	P_E	P_N	Step Score
1	-	-		A disgruntled IT network engineer working for a utility fis dissatisfied with his work environment, due to lack of advancement following his performance review. Due to his feelings of dissatisfaction, he uses his company card over the weekend to purchase personal items. **Upgrade 1**	H	L			**L**
2	-	-		These actions cause him to become paranoid, therefore, he abuses his level of authorized network access on Tuesday of the following week to monitor for any internal communications and discovers that he is the subject of an internal HR investigation. After his discovery, he becomes angry and plans an attack on one of the utility's substations that is adjacent to a busy building supply store. As a part of his attack preparations, he assembles the following tools; personal laptop, handheld ratchet wire cutters, and his issued master key (this master key provides access to all utility substations and is issued to several utility employees). **Upgrade 3, 8**	VH	H			**H**
3	180	180		Next, he conducts a spoofing attack by creating a local VPN admin account using the same name as the HR manager, which then grants him unique capabilities that only the HR manager has authorized access to. Two days following the discovery of the investigation he proceeds to carry out his attack. **Upgrades 3, 8**	VH	VH			**VH**
4	360	540		At the end of the day on Thursday, he exits the main office building at 1730 and drives to the building supply store parking lot (adjacent to the substation) in his personal vehicle to provide concealment and cover near the loading area. He brings with him his personal laptop, handheld ratchet wire cutters and issued master key.	VL	VL			**VL**
5	120	660		While in the vehicle, he opens his laptop and connects to his personal cell phone	VL	VL			**VL**

Table 5.6: Insider Scenario Upgrade Case Example									
Step	**Step Time**	**Cumulative Time**	**Remaining Response Force Time**	**Step Description**	**P_D**	**P_A**	**P_E**	**P_N**	**Step Score**
				hotspot, and logs into the VPN to access the corporate network using the HR director's spoofed account.					
6	120	780		Once in the network he accesses the substation's access control system and disables it, preventing any detection via cameras. **Upgrades 8, 10**	VH	VH			**VH**
7	60	840		He exits his vehicle and walks 50 yards to the west vehicle gate of the substation (adjacent to the building supply parking lot).	VL	VL			**VL**
8	10	850		Using his issued master key, he unlocks the padlock on the vehicle gate, places the padlock into his pocket, and enters through the gate, closing the gate behind him. **Upgrades 11, 14, 15**	VH	VH			**VH**
9	30	880		He walks 25 yards from the gate to the control house building, then uses his key to unlock the deadbolt, swipes his badge at the access panel, and opens the door. **Upgrades 14, 15**	VH	VH			**VH**
10	210	1090		Once inside, he opens all breaker handles and proceeds to cut the main cable coming down the side of the panel with the handheld wire cutters, which results in total loss of control of the substation. **Upgrade 15**	VH	VH			**VH**
11	75	**1165**		He walks out of the control house (leaving the door open behind him), proceeds to the building supply store vehicle gate, walks to his personal vehicle, and leaves the site. **Upgrades 11, 15**	VH	VH			**VH**
								Overall System Effectiveness:	**VH**
Legend: Probability of: PD = Detection; PA = Assessment; PE = Engagement; PN = Neutralization									
Legend: VL = Very Low; L = Low; M = Medium; H = High; VH = Very High									

Table 5.6: Insider Scenario Upgrade Case Assumptions and Notes
Assumptions
Step 2: At this point, the added alerting capability could possibly mitigate the scenario by preventing this action.
Step 10 is where we have to stop the insider from completing the act
All System Changes or Upgrades considered (used in the upgrade scenario)**
1. Program-Procedure // Insider threat awareness training included with annual security refresher training (all staff) (Step 1)
3. D&A // Software that can recognize when an individual is accessing email inappropriately.
8. D&A // Add alerting to administrative/configuration changes to VPN.
10. D&A // Develop security-only network: Segregating IDS and VSS from corporate network and SCADA network.
11. D&A // Cyber key with a master key capability that requires secondary approval for access.

14. D&A // Temporary access release through Dispatch - i.e., personnel visiting the control house would be required to call Dispatch to request access with remote access granted by Dispatch only, which requires additional technical solutions to address loss-of-power and loss of communications scenarios. Could also include a work authorization system, including software, policy, and procedure. Could be restricted to after-hours work only, or when one person is working alone.
**** 15. The two-Person Rule (TPR) is in effect for all network engineers working inside a control building. The second person must be in a similar job position and must maintain line-of-sight of the work being done while inside the control house.**
Notes
Step 2: Procedures are needed to define actions following an alert for this mitigation to be effective.
Step 3: Procedures are needed to define actions following a change to the VPN alert
Step 6: At this step, upgrade #10 eliminates the insider's access to the switch. VH probability of assessment since this action is prevented. System wins.

Outsiders Colluding with Insider Example:

Considerations for Scenario Development

This scenario would follow the same format and sequence as above by using the outsider scenario table. Typically, the team will assume that the outsiders have full knowledge of the site based on the information provided by the insider. The capabilities for each type of adversary are further documented within the DBT. Provided below is a base case scenario for an outsider colluding with an insider. To help differentiate between insider tasks and outsider tasks, it's important to highlight these using two different colors within the table. For example, the color tan represents insider actions and the salmon color represents outsider actions. As reflected in the insider-only example, green indicates where the PPS wins, or that detection AND assessment have occurred. Yellow indicates the step at which the PPS and response must stop the adversary before they complete that step.

Outsider Colluding with Insider Adversary Plan

Provided below is an example of an adversary plan involving an outsider colluding with an insider attack scenario:

Scenario: The SOC operator (insider) has serious financial problems due to a gambling addiction. In early June, the insider is approached by an extremist group (Outsiders) who agreed to pay him $20,000 to cooperate with them by ignoring security alarms. On July 4th at 1345 during peak load, the SOC operator drives through the VECP using his authorized badge access to enter the facility. The SOC operator parks his personal vehicle in the parking lot, exits the vehicle, and walks (100 meters) to the operations building entrance. Using his authorized badge/PIN, he enters the lobby area and moves 75m down the hall to the door of the SOC. He again uses his authorized badge/PIN to enter the SOC. Once he receives the shift briefing from the out-going operator, he logs into the system and begins his 12-hour shift. At 2230, three outsiders park a four-door 4WD pickup truck 25 meters from the Southeastern perimeter.

Outsider 1 stays with the vehicle to serve as a look-out and also to "act" as security. Outsiders 2 and 3 unload weapons (a quarter-pound of explosive door breaching charge, three 1kg of prepared satchel charges, backpacks, and a ladder). Outsiders 2 and 3 move tactically 25 meters to the perimeter fence and prop the ladder against the eight-foot chain link fence. They then move all of the equipment over the fence. From the fence, Outsiders 2 and 3 tactically move 80 meters to the west door of the control house building. They place the quarter-pound explosive door breaching charge and move back around the corner of the building to initiate the charge. After the breach, they move inside the control house. Outsider 2 places two of the 1kg satchel charges on server racks, while Outsider 3 places the third 1kg satchel charge on top of the backup batteries in

the battery bank room. Outsiders 2 and 3 then move to the exterior door, run back to the fence where the ladder is, and proceed over the fence. They both run back to the vehicle and link up with Outsider 1. After all three are loaded into the vehicle, the group command-detonates the three explosive charges and drives away heading south on Carver Street.

Table 5.7: Outsider Colluding with an Insider Scenario Base Case Example

Step	Step Time	Cumulative Time	Remaining Response Force Time	Step Description	P_D	P_A	P_E	P_N	Step Score
1	-	-		The SOC operator (insider) has serious financial problems due to a gambling addiction. In early June, the insider is approached by an extremist group (Outsiders) who agreed to pay him $20,000 to cooperate with them by ignoring security alarms.	-	-			-
2	90	90		On July 4th at 1345 during peak load, the SOC operator drives through the VECP using his authorized badge access to enter the facility.	VH	VL			**VL**
3	120	210		The SOC operator parks his personal vehicle in the parking lot, exits the vehicle, and walks (100 meters) to the operations building entrance.	VL	VL			**VL**
4	120	330		Using his authorized badge/PIN, he enters the lobby area and moves 75m down the hall to the door of the SOC.	VH	VL			**VL**
5	10	340		He again uses his authorized badge/PIN to enter the SOC.	VH	VL			**VL**
6	600	940		Once he receives the shift briefing from the out-going operator, he logs into the system and begins his 12-hour shift.	VH	VL			**VL**
7	15	955		The SOC operator sends secured text through a mobile phone security app.	VH	VL			**VL**
8	-	-	-	At 2230, three outsiders park a four-door 4WD pickup truck 25 meters from the Southeastern perimeter.	VL	VL	VL	VL	**VL**
9	180	1135		Outsider 1 stays with the vehicle to serve as a look-out and also to “act” as security. Outsiders 2 and 3 unload weapons (a quarter-pound of explosive door breaching charge, three 1kg of prepared satchel charges, backpacks, and a ladder).	VL	VL	VL	VL	**VL**
10	45	1180		Outsiders 2 and 3 move tactically 25 meters to the perimeter fence and prop the ladder against the eight-foot chain link fence.	M	M	VL	VL	**VL**
11	120	1300		They then move all of the equipment over the fence.	H	VL	VL	VL	**VL**
12	55	1355		From the fence, Outsiders 2 and 3 tactically move 80 meters to the west door of the control house building. They	VH	VL	VL	VL	**VL**

Table 5.7: Outsider Colluding with an Insider Scenario Base Case Example									
Step	**Step Time**	**Cumulative Time**	**Remaining Response Force Time**	**Step Description**	**P_D**	**P_A**	**P_E**	**P_N**	**Step Score**
				place the quarter-pound explosive door breaching charge and move back around the corner of the building to initiate the charge.					
13	10	1365		After the breach, they move inside the control house.	L	VL	VL	VL	**VL**
14	60	1425		Outsider 2 places two of the 1kg satchel charges on server racks, while Outsider 3 places the third 1kg satchel charge on top of the backup batteries in the battery bank room.	H	VL	VL	VL	**VL**
15	10	1435		Outsiders 2 and 3 then move to the exterior door.	VL	VL	VL	VL	**VL**
16	20	1455		Outsiders 2 and 3 then run back to the fence where the ladder is and proceed over the fence.	VH	VL	VL	VL	**VL**
17	80	1535		Outsiders 2 and 3 run back to the vehicle and link up with Outsider 1.	VL	VL	VL	VL	**VL**
18	30	**1565**		After all three are loaded into the vehicle, the group command detonates the three explosive charges and drives away heading south on Carver Street.	M	L	VL	VL	**VL**
								Overall System Effectiveness:	**VL**
Legend: Probability of: PD = Detection; PA = Assessment; PE = Engagement; PN = Neutralization									
Legend: VL = Very Low; L = Low; M = Medium; H = High; VH = Very High									

Table 5.7: Outsider Colluding with an Insider Scenario Base Case Assumptions and Notes
Assumptions
Steps 8-15: The SOC operator acknowledges all alarms but is not doing anything else until the adversaries have completed their mission.
There were no other employees in the switching yard at the time of the attack.
Satchel charges are set to be command detonated via cell phone.
The explosive breaches inside the control building might be covered by the sound of the fireworks displays in the area.
Step 14: Assessment will be very low from the exterior door camera (100% damaged) from the explosive door breach.
All System Changes or Upgrades considered (used in the upgrade scenario)**
****1: D&A // Two-person rule in the SOC. All alarm notifications annunciate on both operator's displays.**
****2: Response // Four armed onsite responders, rifles, pistols, body armor, trained and performance tested.**
3: Delay // Harden the exterior door to the control building—vault-type door with reinforced frame.
****4: Delay // Anti-cut, anti-climb perimeter fence.**
Notes
The response force timeline is never started since there was no 911 call ever made.
Step 8: has no step time because the vehicle is just arriving near the perimeter.
Step 9: Assessment is very low because the SOC operator is only acknowledging PPS alarms.

Determining Potential Upgrades for the Outsider Colluding with Insider Scenario

After the SEA team validates the outsider colluding with insider base case example, it is time to identify potential upgrades and run one upgrade case to support the scenario (see **Table 5.8** Outsider Colluding with Insider Upgrade Case).

Table 5.8: Outsider Colluding with an Insider Scenario Upgrade Case Example

Step	Step Time(sec)	Cumulative Time (Sec)	Remaining Response Force Time	Step Description	P_D	P_A	P_E	P_N	Step Score
1	-	-		The SOC operator (insider) has serious financial problems due to a gambling addiction. In early June, the insider is approached by an extremist group (Outsiders) who agreed to pay him $20,000 to cooperate with them by ignoring security alarms.					
2	90	90		On July 4th at 1345 during peak load, the SOC operator drives through the VECP using his authorized badge access to enter the facility.	VH	VL			**VL**
3	120	210		The SOC operator parks his personal vehicle in the parking lot, exits the vehicle, and walks (100 meters) to the operations building entrance.	VL	VL			**VL**
4	120	330		Using his authorized badge/PIN, he enters the lobby area and moves 75m down the hall to the door of the SOC.	VH	VL			**VL**
5	10	340		He again uses his authorized badge/PIN to enter the SOC.	VH	VL			**VL**
6	600	940		Once he receives the shift briefing from the outgoing operator, he logs into the system and begins his 12-hour shift. **Upgrade 1**	VH	M			**M**
7	15	955		The SOC operator sends secured text through a mobile phone security app.	VH	VL			**VL**
8	-	-		At 2230, three outsiders park a four-door 4WD pickup truck 25 meters from the Southeastern perimeter.	VL	VL	VL	VL	**VL**
9	180	1135		Outsider 1 stays with the vehicle to serve as a lookout and also to "act" as security. Outsiders 2 and 3 unload weapons (quarter-pound of explosive door breaching charge, three 1kg of prepared satchel charges, backpacks, and a ladder).	VL	VL	VL	VL	**VL**
10	45	1180	**1065**	Outsiders 2 and 3 move tactically 25 meters to the perimeter fence and prop the ladder against the eight-foot chain link fence. **Upgrade 1**	VH	VH	VL	VL	**VL**
11	1320	2485	Plus 55	They then move all of the equipment over the fence. **Upgrade 1, 4** (New fence delay time adds 20 min)	VH	VH	VH	H	**H**

Table 5.8: Outsider Colluding with an Insider Scenario Upgrade Case Example									
Step	**Step Time(sec)**	**Cumulative Time (Sec)**	**Remaining Response Force Time**	**Step Description**	**P_D**	**P_A**	**P_E**	**P_N**	**Step Score**
12	55	2540		From the fence, Outsiders 2 and 3 tactically move 80 meters to the west door of the control house building. They place the quarter-pound explosive door breaching charge and move back around the corner of the building to initiate the charge.					
13	10	2550		After the breach, they move inside the control house. **Upgrade 3**					
14	60	2610		Outsider 2 places two of the 1kg satchel charges on server racks, while Outsider 3 places the third 1kg satchel charge on top of the backup batteries in the battery bank room.					
15	10	2620		Outsiders 2 and 3 then move to the exterior door.					
16	20	2640		Outsiders 2 and 3 then run back to the fence where the ladder is and proceed over the fence.					
17	80	2720		Outsiders 2 and 3 run back to the vehicle and link up with Outsider 1.					
18	30	**2750**		After all three are loaded into the vehicle, the group command detonates the three explosive charges and drives away heading south on Carver Street.					
								Overall System Effectiveness:	**H**
Legend: Probability of: PD = Detection; PA = Assessment; PE = Engagement; PN = Neutralization									
Legend: VL = Very Low; L = Low; M = Medium; H = High; VH = Very High									

Table 5.8: Outsider Colluding with an Insider Scenario Upgrade Case Assumptions and Notes
Assumptions
Step 8: SOC operators (via two-person rule - upgrade 1) see the alarms, assess VSS input, and call response force.
Step 11: The response force engages outsiders and stops them before they get through the fence.
All System Changes or Upgrades considered (used in the upgrade scenario)**
****1: (Detection and Assessment) - Two-person rule in the SOC. All alarm notifications annunciate on both operators' displays**
2: (Response) - Four armed onsite responders, rifles, pistols, body armor, trained and performance tested.
****3: (Delay) - Harden the exterior door to the control building—vault-type door with reinforced frame.**
****4: (Delay) - Anti-cut, anti-climb perimeter fence (adds fence delay time of 20 min – 1200 seconds).**
Notes
Step 11: System wins
Upgrade 3: No longer needed since in Step 11 **Upgrades 1 and 4** defeat the adversary.

Chapter 6: Performance Testing

Performance Testing

The speed at which knowledgeable adversaries could attack a facility and damage vital equipment could negate the effectiveness of PPS components and the responder's actions. Barriers may not provide sufficient delay time for an effective off-site response. Therefore, a team should conduct performance testing to ensure a timely and effective response during the critical early stages of an attack. Periodic PPS testing that includes the off-site (emergency responders) helps establish and maintain the effectiveness of such a response. It is also used as a tool to develop, correct, or modify physical protection strategies.

Performance testing has a single purpose: to determine how well a tested subject (people, procedures, equipment, or system) functions. The results provide three significant elements of information:

- Whether the team adequately performed the required functions
- Whether the performance metric used in the analysis is accurate and represents "real-world" conditions
- Areas of weakness or substandard performance that can be improved

A valid assessment of PPS components and responders' capabilities cannot be made solely by reviewing documents and other information about location, numbers, training, procedures, and equipment, among others. Regardless of what a response looks like on paper, a team must performance-test and validate it.

To determine whether a sensor or responder can perform as required, the managers must see it in action. Responders must demonstrate that they can perform their routine and emergency duties by performing those duties in real-world conditions. They must also operationally test detection equipment reliability and suitability in a realistic environment. Some performance characteristics can be observed under actual conditions; however, chance does not allow the spontaneous observation of sufficient routine and emergency functions. That is when performance testing is required.

A functional test of a sensor (turning off or on) is not a performance test. Physically moving into the sensor envelopes at different angles, levels, and speeds are adequate performance tests. By using an "attempt-to-defeat" methodology, the performance testing process is much more effective and provides the "worst-case" performance metric.

Performance tests range in complexity from limited-scope demonstrations of a single individual skill or sensor to an integrated response with other elements of a facility's PPS and overall security posture. An alarm response performance test is typically conducted with no prior notice to evaluate a true response to a specific location. Alarm response performance test scenarios must be based on simulated adversary actions consistent with the DBT and site-specific vulnerability assessments. The purpose of this testing is to evaluate the responder's timely and effective response to various alarm conditions. These tests must take into consideration all aspects of the response; including communication, movement times, personnel protective measures, equipment availability and serviceability, and any facility coordination activities that may be necessary for effective mitigation of a security incident.

Alarm response performance tests must be coordinated with site representatives and trusted agents to ensure that safety requirements are fulfilled, security is not compromised, and operational disruption is minimized. Upon commencement of an alarm response performance test, responding personnel must be advised of the test

so they can be available for real-world emergencies if needed. Performance testing of PPS functions does require notification to the alarm monitoring organization so an actual response does not happen.

Planning is important to any performance test. No matter how simple or complex the test is, the planners must determine who participates, and the scope, reason, time, and location of the test before they can execute the test properly. A designated test planner should be assigned with the ultimate responsibility for planning to ensure that the team will meet the test objective(s) through a fair and realistic test. Including response personnel within the exercise planning and evaluation process reinforces the value and importance of an effective response. It also affords the test planner additional perspectives that can result in improvements in the performance of the PPS.

Performance testing can supply a security manager with a great deal of information on the ability of the PPS and responders to meet the DBT. However, unless they are conducted realistically and with a well-written plan, they may not achieve their desired objectives.

Below is an example of a series of alarm response performance tests to gather an accurate off-site response time:

The Deputy Sheriff's response time is measured from the initial alarm annunciation to arrival on scene (the worst case is the longest response time of 20 minutes and 3 seconds).

- Test 1 Day 8:00 a.m.: 13 minutes, 46 seconds
- Test 2 Day 12:00 p.m.: 17 minutes, 22 seconds
- Test 3 Day 5:00 p.m.: 20 minutes, 3 seconds
- Test 4 Night 9:00 p.m.: 18 minutes, 39 seconds
- Test 4 Night 02:00 a.m.: 12 minutes, 12 seconds
- Test 6 Night 5:00 a.m.: 14 minutes, 44 seconds

The performance tests would not normally provide initial notification to capture the most realistic times. Use the worst-case time for the response time in the SEA scenario. The response time of 20 minutes and 3 seconds for the off-site response would stand until additional performance testing data could validate different times.

Concluding Notes

This guide is intended to help frame a process by which physical protection experts within a company or utility can assess the effectiveness of their facility's protection system. The DBT provides the parameters of the threat against which an organization must be protected. The VISA process is a simple method to apply the DBT and assess the overall system's effectiveness at thwarting the postulated threat. Many methods to apply a DBT exist, but this approach has proven to be simple, straightforward, and effective when considering an industrial target. The E-ISAC Physical Security Advisory Group's (PSAG) objective in this effort is to provide a useful and effective tool for industry. Feedback to the PSAG is appreciated and can be provided to the E-ISAC at physicalsecurity@eisac.com.

Disclaimer

This guide was originally prepared by the Pacific Northwest National Laboratory (PNNL) for the U.S. Department of Energy and has been updated by the Electricity Information Sharing and Analysis Center's (E-ISAC's) Physical Security Advisory Group (PSAG).

This guide is provided on an "as-is" and "as available" basis. The use of the guide is entirely voluntary and at the sole risk of the user. The North American Electric Reliability Corporation (NERC), which is the operator of the E-ISAC, does not make any warranty, express or implied, or assume any legal liability or responsibility for the; accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represent that its use would not infringe on privately-owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by NERC. You knowingly and freely assume all risk when using this guide. You, on behalf of yourself and your personal representatives, and/or agents, and your business, agree to release, waive, discharge, hold harmless, defend, and indemnify NERC from any damages, costs, claims, actions, or losses, however arising, from your use of this guide.

Appendix A: Sample Worksheets

The following blank worksheets are samples that teams can use and modify.

Table A.1: Sample System Effectiveness Worksheet (Outsider Threat)

Step	Step Time[(a)]	Cumulative Time[(a)]	Remaining Response Time[(a)]	Step Description	P_D	P_A	P_E	P_N	**Step Score**
								Overall System Effectiveness	

(a) Time is in seconds, H = high, L = low, M = medium, P_A = probability of assessment, P_D = probability of detection, P_E = probability of engagement, P_N = probability of neutralization, VH = very high, VL = very low

Table A.2: Sample System Effectiveness Worksheet (Insider Threat)				
Step	**Step Description**	**P_D**	**P_A**	**Step Score**
			Overall System Effectiveness	
H = high, L = low, M = medium, P_A = probability of assessment, P_D = probability of detection, VH = very high, VL = very low				

Appendix B: Design Basis Threat Acronyms

AOO	Asset Owners and Operators
APL	Asset Protection Level
DBT	Design Basis Threat
DVE	Domestic Violent Extremist
EFP	Explosively-Formed Projectile
H	High
IDS	Intrusion Detection System
IED	Improvised Explosive Device
L	Low
M	Medium
OSE	Overall System Effectiveness
P_a	Probability of Assessment
P_d	Probability of Detection
P_e	Probability of Engagement
P_n	Probability of Neutralization
PPS	Physical Protection System
PSAG	Physical Security Advisory Group
SEA	System Effectiveness Analysis
SME	Subject Matter Expert
SOC	Security Operations Center
TPR	Two-Person Rule
TLP	Traffic Light Protocol
VBIED	Vehicle-Borne Improvised Explosive Device
VECP	Vehicle Entry Control Point
VH	Very high
VISA	Vulnerability of Integrated Security Analysis
VL	Very Low
VMD	Video Motion Detection

Appendix C: Movement Table (Metric)

	10 seconds		*30 seconds*		*60 seconds*	
	Personnel	***Vehicle***	***Personnel***	***Vehicle***	***Personnel***	***Vehicle***
Slow	**6 m** *2 Km/h (Crawling or crouch)*	**28 m** *10 Km/h*	**17 m** *2 Km/h (Crawling or crouch)*	**83 m** *10 Km/h*	**33 m** *2 Km/h (Crawling or crouch)*	**167 m** *10 Km/h*
Medium	**14 m** *5 Km/h (Tactical Movement)*	**133 m** *48 Km/h*	**42 m** *5 Km/h (Tactical Movement)*	**400 m** *48 Km/h*	**83 m** *5 Km/h (Tactical Movement)*	**800 m** *48 Km/h*
Fast	**28 m** *10 Km/h (Running)*	**269 m** *97 Km/h*	**83 m** *10 Km/h (Running)*	**808 m** *97 Km/h*	**167 m** *10 Km/h (Running)*	**1616 m** *97 Km/h*
Very Fast	**n/a**	**402 m** *145 Km/h*	**n/a**	**1208 m** *145 Km/h*	**n/a**	**2416 m** *145 Km/h*

Appendix D: Movement Table (Imperial)

	10 seconds		*30 seconds*		*60 seconds*	
	Personnel	***Vehicle***	***Personnel***	***Vehicle***	***Personnel***	***Vehicle***
Slow	**5 yd** *1 mph* *(Crawling or crouch)*	**30 yd** *6 mph*	**15 yd** *1 mph* *(Crawling or crouch)*	**88 yd** *6 mph*	**30 yd** *1 mph* *(Crawling or crouch)*	**176 yd** *6 mph*
Medium	**15 yd** *3 mph* *(Tactical Movement)*	**147 yd** *30 mph*	**44 yd** *3 mph* *(Tactical Movement)*	**440 yd** *30 mph*	**88 yd** *3 mph* *(Tactical Movement)*	**880 yd** *30 mph*
Fast	**30 yd** *6 mph* *(Running)*	**293 yd** *60 mph*	**88 yd** *6 mph* *(Running)*	**880 yd** *60 mph*	**176 yd** *6 mph* *(Running)*	**1760 yd** *60 mph*
Very Fast	**n/a**	**440 yd** *90 mph*	**n/a**	**1320 yd** *90 mph*	**n/a**	**2640 yd** *90 mph*