Jail Vulnerability Assessment: A Systems Approach to Improve Safety and Security

FINAL DRAFT

December 2008

[inside front cover]

U.S. Department of Justice
National Institute of Corrections
320 First Street, NW
Washington, DC 20534

National Institute of Corrections
World Wide Web Site
www.nicic.org

[title page]

Jail Vulnerability Assessment: A Systems Approach to Improve Safety and Security

Rod Miller
John E. Wetzel

December 2008

NIC Accession Number 000000

[verso title page]

This document is supported by cooperative agreement #07J61GJS0 from the National Institute of Corrections, U.S. Department of Justice. Points of view or opinions stated in this document are those of the authors and do not necessarily represent the official opinion or policies of the U.S. Department of Justice.

CONTENTS

Foreward

[To be developed with NIC editors to their specifications.]

Acknowledgements

This document builds on the work of Sandia National Laboratories (SNL) Security Systems and Technology Center: Chris E. Robertson, Ivan G. Waddoups and Michael S. Pacheco. The Pennsylvania Department of Corrections adapted the SNL work for use in state prisons, through the efforts of Eugene J. Brannigan, John Bihun and Michael D. Klopotoski.

The American Correctional Association (ACA) developed the first Correctional Vulnerability Assessment Handbook with funding from the National Institute of Justice. The ACA team was led by Robert J. Verdeyen, and included J. T. O'Brien, Pat Keohane, Tim LeMaster, Don Romine, David Sweetin, George Wagner, and Rod Miller. The Colorado Department of Corrections further refined the correctional VA process through the efforts of Lou Archuleta and Michael Fowler.

Several jails advanced the development of vulnerability assessment tools and techniques for jails by hosting training programs: Clark County, Nevada; Alexandria, Virginia; Davidson County, Tennessee; and Madison County (Huntsville), Alabama. Several sites provided opportunities to field test the jail methodology: Franklin County PA; Marion County IN, and Dona Ana County NM.

Mark Martin provided valuable guidance and advice throughout the development of his handbook. Randall S. Wylie, Tim Albin, Scott Bickford, Curtis Flowers and James Nabors offered comments after reviewing the first draft.

INTRODUCTION

The National Institute of Corrections (NIC) funded this document to provide a new resource to jails as they strive to operate safe and secure facilities. Another new NIC publication, ***Guide to Effective Risk Management in Jails,***[1] examines a broader range of risks that may affect an organization's ability to achieve its mission, describes the risk management process and provides guidance to jail officials who want to establish formal risk management programs. This handbook offers new methods and tools to improve jail safety and security.

Purpose and Scope

This document builds on the resources that were developed for prisons by the American Correctional Association (ACA) with funding from the National Institute of Justice (NIJ).[2] As the prison materials were used to train jails, it became clear that adapting them for use in jails requires substantial revisions and the development of new tools.

This manual and its associated resources balance the depth of analysis that is provided by the prison process with the breadth of scope and participation that is needed in the jail setting. It is based on several principles that have proven effective in the jail setting:

1. <u>Participation</u>. Engaging many stakeholders in the process improves the outcomes and provides many secondary benefits.
2. <u>Varied perspectives</u>. Involving many types of participants provides needed perspectives. Every participant sees different angles and poses unique questions.
3. <u>Expertise is found at all levels</u>. Every stakeholder, from line staff to administrators, brings experience and expertise that are essential to the success of the process.
4. <u>Continuous Process</u>. Maintaining safety and security is a continuous process. The chain of safety and security is only as strong as its weakest link.

Practitioners might recognize several of these principles because they ground many of NIC's initiatives. This document identifies other NIC resources that will aid participants.

Audience and Intended Uses

This document and its associated resources have the primary goals of:

- Improving jail safety and security
- Promoting the development and implementation of *continuous* safety and security improvement practices

---

[1] Martin, Mark, and Claire Lee Reiss. *Guide to Effective Risk Management in Jails.* National Institute of Corrections, U.S. Department of Justice. Washington D.C. 2008.
[2] Miller, Rod, Robert J. Verdeyen, J.T. O'Brien, and Donald Romine. *Correctional Vulnerability (CVA) Handbook, Final Draft*. American Correctional Association, Alexandria VA. 2006. Funded by the National Institute of Justice, U.S. Department of Justice.

To those ends, *jail operators* are the primary audience: from line staff to top administrators. Their continuous efforts are required to maintain safety and security under increasingly challenging conditions. All participants in the jail vulnerability assessment process will acquire new knowledge, skills and insights that will help them better perform their duties. Additional benefits will vary:

- *Line staff* will find a new voice to contribute their concerns and suggestions to improvement efforts.
- *First line supervisors* will have new tools to provide to line staff to enhance their effectiveness.
- *Managers* will create new mechanisms to engage subordinates in improvement efforts and new communication channels to identify evolving concerns.
- *Administrators* will find new insights into daily operations and will develop new information to share with policymakers and funding sources.
- *Trainers* will have new tools to improve employee initial and in-service training and new information about actual practices on the floor compared to intended practices.
- *Policy and procedure developers* will learn how their directives are being implemented and instances in which directions are creating problems.
- *Civilian employees* will find new ways to promote safety and security and new opportunities to voice their concerns.
- *Program providers* will learn about the impact of their activities on overall safety and security and have new opportunities to share their ideas with others.
- *Maintenance personnel* will understand the impact of facility and equipment conditions on safety and security and secure new insights into maintenance needs.
- *Contractors* will learn about the interface between their activities and facility security, and will have new opportunities to contribute to improvement efforts.

Although the primary users of this material are involved with daily jail operations, many other stakeholders will find benefits, including:

- Sheriffs
- County commissioners/supervisors
- Budget and finance officials
- Risk managers
- Insurance providers
- Inspection officials
- Employee labor organizations

There are other parties who may benefit from the methods and tools in this document. As the jail vulnerability assessment methodology has evolved and has been tested in the field, participants have found that the benefits accrue in direct relation to the effort put into the process.

CHAPTER 1: SETTING THE STAGE

Making the most of this document and its related resources begins with understanding the broader context in which jails operate.

A. Safety and Security Principles

Safety and security are the foundation on which all jail operations must be built.

Without effective, continuous safety and security practices, everyone is exposed to a variety of risks. Programs and services are often part of a jail's mission, but these must be built on a strong foundation.

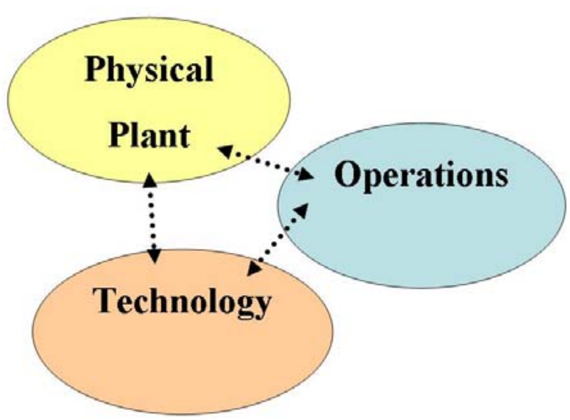
Security is not convenient.

Implementing security practices requires time and attention and usually slows the pace of operations. Employees often suspend basic security practices in order to accommodate what they perceive to be the needs of some jail stakeholders. This might take the form of propping a secure movement door open or failing to positively identify someone before allowing access to an area. Such well-intentioned actions seriously undermine facility safety and security. Such practices fall under the maxim "The road to Hell is paved with good intentions."

Achieving safety and security requires balancing facilities, technology, and operations.

All three jail components of the jail setting must be sufficient and balanced in order to achieve and maintain safety and security. This document explores all three dimensions and provides tools to help assess and improve each one, and all three together.

Figure 1.1: Three Components of Jail Safety and Security



Proper staffing is essential.

Maintaining safety and security demands sufficient staff who are:

- Qualified
- Directed by policies and procedures
- Properly trained
- Effectively supervised
- Properly deployed (at the right place, at the right time)

NIC has developed extensive staffing analysis resources which should be consulted.

B. Courts and the Constitution

Court decisions define important parameters for jail operations by establishing minimum levels of service, performance objectives, prohibited practices, and specific required practices. State and local courts also play an active role in evaluating and guiding jail operations.

Decisions handed down by federal courts have required jails to:

- Protect inmates from themselves, other inmates, staff and other threats
- Maintain communication with inmates and regularly visit occupied areas
- Respond to inmate calls for assistance
- Classify and separate inmates
- Ensure the safety of staff and inmates at all times
- Make special provisions for processing and supervising female inmates
- Deliver all required inmate activities, services, and programs (medical, mental health, exercise, visits, etc.)
- Provide properly trained staff

Federal court involvement with jails goes back more than 40 years. State and federal prisons were the focus of many landmark cases in this era, and local jails soon became targets as well. Early federal decisions tackled fundamental constitutional issues in jails. Many of these pioneering decisions are still cited in current litigation.

The United States Constitution imposes an extraordinary "duty to protect" on jails that has no counterpart in public safety. [3] While the jail duty is less visible to the public, and likely less appreciated, it rises above the constitutional responsibilities of public safety agencies. Even probation does not approach the duty to protect that is imposed on jails. Probation officials are not held responsible for the behavior of offenders under their supervision, nor for what happens to the offenders when they are not actually with a probation officer.

[3] When fire, police and other public safety personnel provide services, the Constitution certainly comes into play, establishing many requirements for the manner in which services are delivered. But in these cases, the duty to protect commences when officials decide to act.

A jail's duty to protect is constant, beginning when an inmate is admitted and continuing until release. Caselaw clearly establishes the responsibility of jail officials to protect inmates from a "risk of serious harm" at all times, and from all types of harm-- from others, from themselves, from the jail setting, from disease, and more.

Officials may be found to be "deliberately indifferent" if they fail to address a known risk of serious harm or even if they *should* have known of the risk. Ignorance is not a defense. Failure to protect inmates may result in liability. Usually court intervention takes the form of orders that restrict or direct jail practices. Sometimes the courts award compensatory damages to make reparations to the plaintiffs. In more extreme situations, defendant agencies may be ordered to pay punitive damages. A U.S. Supreme Court decision held that punitive damages may even be assessed against individual defendants when indifference is demonstrated.

Federal courts have made it clear that lack of funds does not excuse violation of inmates' constitutional rights:

> *Humane considerations and constitutional requirements are not, in this day, to be measured or limited by dollar considerations… Jackson v. Bishop,* 404 F.2d 571 580 (8th Cir.1968)

Operating a jail is a tremendous responsibility. Courts continue to define responsibilities in light of constitutional requirements. Proactive jail managers are informed by evolving caselaw and attempt to ensure that all aspects of their operation are in compliance. Responsible elected officials respect their constitutional duty to protect jail inmates and staff, and find ways to fund jail staffing and operations.

C. Standards

Standards and court decisions are closely linked. In many instances the courts *defer to* standards, while in other cases standards are often *based on* court decisions.

Most jails are, in effect, "owned" by elected county officials (usually county commissioners) who have fiscal authority. But most jails are *operated* by sheriffs, who are also elected county officials. Sheriffs share responsibility for jail operations with county commissioners. This shared responsibility often creates conflicts and challenges at the local level.

When jail conditions or operations fall below constitutional requirements, federal courts may step in and order improvements. State courts may also intervene when there are violations of state law or the state constitution. Courts set boundaries for jails in response to specific circumstances that are brought to their attention by plaintiffs. In this manner, the guidance provided by the courts is somewhat hit or miss. Courts usually provide a "yes or no" answer to the question "is this practice or condition acceptable in the context of this case?" Sometimes courts will give a hint of what is acceptable in the form of remedial orders that give specific instructions, but not always.

Letting courts determine jail requirements is expensive for all parties, and does not produce comprehensive guidance for jail operations.

Mandatory State Standards

In this context, many states found it necessary to attempt to regulate jail conditions and operations by adopting minimum jail standards. In most instances, states also had enforcement authority to compel compliance. As of 2007, 27 states had some form of state jail standards that were administered by a state agency or commission.[4]

State jail standards are usually described as "minimum" standards. They attempt to establish practices and conditions that the courts will find acceptable and which represent basic appropriate levels founded on prevailing professional opinion.

As states stepped up to the plate and became involved with regulating jail conditions, litigants found another party to name in suits. States became co-defendants based on the theory that the state had a duty to identify jail deficiencies, and in many states, the authority to compel compliance. Litigants argued, often successfully, that states were jointly liable for substandard jail conditions. As a result of such liability, some states have backed away from enforcement.

Voluntary State Standards

Five states (Florida, Idaho, Montana, Oregon, and Utah) have adopted voluntary standards and implement peer audits or reviews. For example, the Idaho Sheriffs' Association adopted comprehensive voluntary jail standards in 1990. Volunteer peer inspectors implement annual inspections, which are coordinated by the association.

Professional Standards

While many state jail standards represent minimums, national standards written by the American Correctional Association (ACA) describe a higher "professional" level of standards and practices. Compliance with ACA standards is voluntary. Although ACA offers accreditation to local jails, less than five percent of all jails are currently accredited.

Many, if not most, state jail standards are based in part on the ACA standards. Recently, county sheriffs and commissioners in Montana used the ACA Adult Local Detention Facility (ALDF) standards as the starting point for the development of their new voluntary standards.

ACA has developed innovative new "performance standards" that describe the conditions to be achieved, followed by a series of "expected practices" that identify activities to be implemented and conditions to be maintained.

There are seven functional areas in the *ACA Performance Based Standards for Adult Local Detention Facilities*[5] as shown in Figure 1.2.

---

[4] Jail Standards and Inspection Programs. Mark D. Martin. National Institute of Corrections, U.S. Department of Justice. Washington, D.C. April 2007

[5] American Correctional Association in cooperation with the Commission on Accreditation for Corrections, *Performance-Based Standards for Adult Local Detention Facilities*, *Fourth Edition*, (Maryland: American Correctional Association, 2004)

Figure 1.2: Functional Areas for ACA Jail Standards

1. **Safety** -- Maintain a safe living and working environment
2. **Security** -- Protect community, staff, and inmates from harm
3. **Order** -- Maintain order and manage behavior
4. **Care** -- Provide for inmates basic needs
5. **Program and Activity** -- Keep inmates productively occupied and promote successful return to community
6. **Justice** -- Fair treatment and respect of inmate rights and also maintain accountability for behavior
7. **Administration and Management** -- Professional and responsible management consistent with legal requirements

<u>ACA's New "Core Jail Standards"</u>

With the assistance of the National Institute of Corrections, ACA developed draft cort jail standards in 2007. According to ACA, the core standards are similar in scope and content to state jail standards and fill a need for jails that operate without any state standards, along with any jails interested in compliance with national standards. The core standards attempt to describe the basic practices and conditions that all jails should maintain. ACA believes that any jail failing to achieve compliance with core standards is at risk for future litigation and other problems. More important, failure to comply with core standards may expose staff, inmates, contractors, visitors, and others to risks within the work environment.

ACA adopted Core Jail Standards in January 2009. Appendix J presents excerpts from these standards. The excerpts identify issues and practices that are related to facility safety and security. This document and its related resources rely on the ACA ALDF and Core standards. Many of the checklists and other tools integrate key ACA standards and practices.

D. Trends in the Jail Setting

Jails are dynamic settings that face change on all fronts. Maintaining safety and security demands acute awareness of the evolving context. Each jail presents its own constellation of physical, technology and operational challenges. At a national training event in 2008, participants from nine counties identified the following trends in their jails.

Figure 1.3: Changes Reported by Jail Managers

<u>Facilities</u>

- Although there is some new construction, "new" is not necessarily better
- Crowding is common in most jails
- Aging facilities
- Condition deteriorating from lack of maintenance and repair
- Poor design
- More jails converted from other uses (e.g. hospital, mental hospital)
- Facilities designed for lower security inmates are being used for higher security

Technology

- Has improved and is sometimes less expensive than before
- Often inappropriately used instead of staff, rather than to enhance staff performance
- Extensive use of closed circuit television (CCTV)
- Increased recording of inmate and staff activities
- High-tech systems, such as hand-held PDA and touch screens (which often break)
- Some new technology fosters staff complacency (over-reliance)
- Costs sometimes prohibit acquiring technology that would enhance safety
- Continuing confusion about the difference between "observation" and "supervision"

Operations

Inmates

- Younger and older
- More violent
- Increasing number of inmates with mental health needs
- More medical needs
- More gangs
- Increasing ethnic and racial diversity
- More predatory inmates
- Fewer "good" inmates
- More women

Staffing

- Increasing turnover
- Lower retention rates
- High rate of retirement
- Eroding work ethic with younger employees
- Generational issues and challenges
- Difficulties with recruiting and screening
- Current work force is "worn out"
- Employee tenure is decreasing
- New employees have misconceptions about the jail and their job
- More difficulty delivering effective training

Funding

- More competition with other agencies for operating funds
- Sometimes encounter hiring "slow downs" or freezes
- Often not allocated funds that are requested

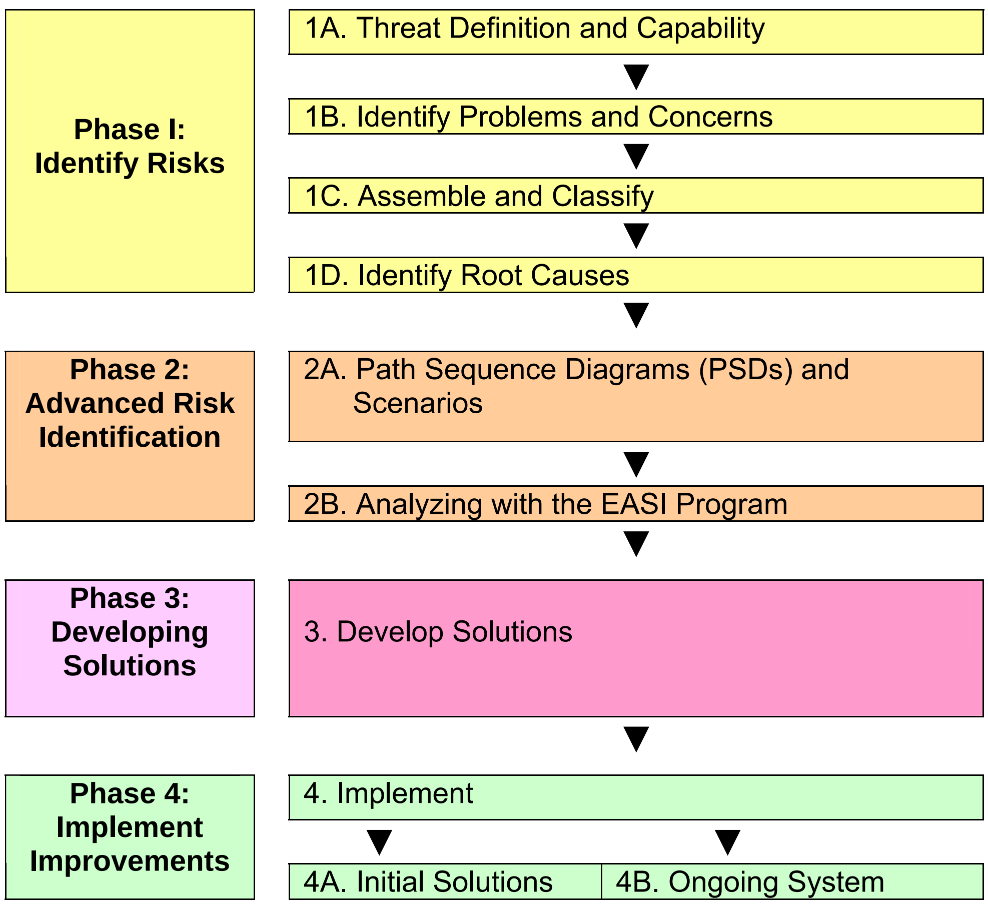
The preceding list presents *some* of the changes that challenge jails and their operators. Many of these changes are incremental and are not fully appreciated by jail personnel as they occur. Therefore, it is important to step back and look back to identify the changes that have been encountered as a prelude to the jail vulnerability assessment process.

E. The Jail Vulnerability Assessment (JVA) Process

The JVA process described in this document is comprised of four phases of activity. The first three phases examine every facet of the jail setting, identifying problems and concerns, corresponding causes, and solutions. The fourth and final phase sets the stage for ongoing, continuous activities.

Figure 1.4 presents the four phases and the steps that comprise each. The process is comprised of a series of *consecutive* steps, each building on the preceding activities. To realize the most value from the process, all steps should be completed in order. However, individual phases or even individual steps may prove useful to address specific issues or problems, if it is not feasible to implement the entire process.

Figure 1.4: Jail Vulnerability Assessment Process



Each phase of work is described briefly in the following narrative. Chapters Two through Five present detailed instructions for each step.

Phase One: Identify Risks

1A. Threat Definition and Capabilities

A clear understanding and prioritization of threats is the starting point for the process. Each facility will have its own unique constellation of threats that are of concern. These threats, and their priority are likely to change over time.

Without a clear definition of threats, it is difficult to assess the adequacy of facilities, technology or operations. For example, if escape is not an issue, as might be the case in work release facility, many of the physical, technical, or operational features will not be of concern. On the other hand, a specific type of security door or lock might pose a risk in a facility that defines escapes as a primary threat. Figure 1.5 depicts a simple decision tree.

Figure 1.5: Defining Risks Based on Threats

Determining the *capabilities* of priority threats is also a requisite for determining if facilities, technology or operations pose a risk. For example, in many jails the small windows in inmate cells are the exterior security perimeter of the facility. If this facility feature is compromised, there is nothing between the inmate and the outside world. If “introduction of contraband” is defined as a priority threat, then an inmate’s ability to compromise the window, or the capabilities of an outside accomplice, are of great concern.

Whether or not the window is vulnerable will be affected by the inmate’s (threat’s) capabilities. If the inmate has assistance from the outside, the risk of window penetration is heightened. If the inmate has access to certain tools or materials that may be used as tools, the risk is also higher. In this manner, threat capabilities help determine the level of risk.

1B. Identify Problems and Concerns

During this step, all facets of the facility, technology and operations are compared to threats and threat capabilities. Through a series of targeted activities, and using several analytical tools, the jail will be viewed from a variety of perspectives. This step casts a wide net to identify the full range of problems and concerns, involving many stakeholders in varied roles. This is not a security audit or inventory; rather it assesses features in the context of the specified threats. It determines if a feature is *effective* against the threat. Instead of describing the characteristics of a door lock or confirming that it is operational, the lock is evaluated in terms of threats and threat capabilities.

1C. Assemble Problems and Concerns and Classify

The preceding step identifies many problems and concerns, some of which are freestanding and not seemingly connected to others. In this step, findings are sorted and classified according into three categories: facility, technology and operations. This initial sorting helps to group problems with similar characteristics, a step toward finding effective solutions.

1D. Identify Root Causes

After the initial findings have been re-sorted according to their characteristics, the "root causes" are identified. Deficiencies and problems that have been identified are usually symptoms of underlying problems. This step of the process examines the cause, or causes, of each problem, setting the stage for formulating effective solutions..

For example, one of the findings might be that "booking officers are not following procedures regarding security of inmates during initial processing." Failing to consistently follow procedures could be considered a symptom. In this case, the root cause might be:

- Inadequate *policies and procedures* (officers are not properly directed in writing)
- Inadequate *training* (the procedure is adequate but officers are not properly trained to implement it)
- Lack of employee *supervision* (officers know how to act properly but their behavior is not consistently reinforced by effective first line supervision)

There might be more potential root causes for the deficiency. Step 1D determines what causes the deficiency so that corrective action may be taken. <u>*Note*</u>. Some of the problems and deficiencies in this first phase of the process might warrant immediate attention, which is taken concurrent with moving on to the next phase of the process.

<u>Phase Two: Advanced Risk Identification</u>

This phase of the process uses powerful new techniques and tools to dig deeper into risks and vulnerabilities. These tools make it possible to actually *calculate* the probability of threat scenario's success. This phase of the process centers on the "EASI"[6] methodology developed by Sandia National Laboratories. First used to protect weapons systems and nuclear assets, the EASI methodology has been successfully applied to prisons and is now integrated into the jail vulnerability assessment process.

2A. Develop Path Sequence Diagrams and Scenarios

This step produces several scenarios (series of actions) that exploit weaknesses in the facility, technology, and operations. The steps are illustrated in "path sequence diagrams" (PSD) as graphic representations of facility features. PSD's set the stage for collecting data about detection, delay and response. Several scenarios are developed; data are collected by implementing each step and recording the findings. The data are recorded for use in the next step.

2B. Analyzing with the EASI Program

The scenarios developed in the preceding step, and the corresponding data, are entered into the Excel-based EASI program. EASI uses sophisticated formulas to calculate the probability of a threat's success. Better yet, the EASI program calculates the impact of potential solutions, modeling the value of the various potential solutions to ensure that the most effective actions are selected.

Phase Three: Develop Solutions

The findings from Phase One and Phase Two are combined at this point in the process. Root causes are analyzed, leading to the identification of specific solutions, or, more accurately, "solution sets" that will reduce risk.

Phase Four: Implement Improvements

The solutions are implemented in this final phase, and an ongoing safety and security improvement program is developed.

4A. Implement Initial Solutions

Many specific issues will be identified the first time a JVA is conducted. Most of these will be addressed in the implementation phase, correcting the underlying causes. It is not unusual for a wide spectrum of improvements to be implemented at this point.

4B. Implement an Ongoing System

Maintaining a safe and secure jail requires continuous effort. Changes in facilities, technology, and operations must be identified and appropriate responses must be implemented. This final step in the JVA process develops an ongoing system that provides "continuous safety and security improvement."

---

[6] Estimate of Adversarial Risk Interruption.

CHAPTER 2: Phase One of the JVA Process

Introduction

The first phase of the JVA process guides participants through a critical examination of all aspects of the facility and its operation. This examination will compare current facilities, technology, and operations to the specific threats that are identified in Step 1A. You will describe the capabilities that your adversaries possess.

The examination will involve a series of excursions into the facility, each time focusing on a new perspective. Six dimensions will be explored:

Elements of Safety and Security

1. Facilities
2. Technology
3. Operations

Elements of Physical Protection Systems

4. Detection
5. Delay
6. Response

At the end of this phase, all findings will be assembled and classified, and the causes of the deficiencies will be explored.

A. Step 1A: Defining Threats and Threat Capabilities

Step 1A requires a careful consideration of the risks that are of concern to you, your colleagues, and other stakeholders. There are many potential threats to the safety and security of a jail. Threat definition is the foundation on which the vulnerability assessment is built. A feature of your facility, such as a cell lock, may be of great concern if you have defined escape as a threat. The same lock, located in a low security setting in which escape is not a threat, will not raise alarms. This process hinges on clear definition of threats.

Defining Threats

To start this process, ask yourself "What problems or events do I want to prevent?" Develop a list. Ask other stakeholders the same question--the answers may surprise you. Sheriffs, county commissioners, budget officials, law enforcement agencies and other stakeholders should be asked to express their concerns at this point in the process.

After you have compiled an initial list, narrow it down or categorize it into threats. Although Merriam Webster defines a threat as *"an indication of something impending,"* in the jail context a threat is defined in terms of events and activities that are to be prevented or avoided.

As a starting point, review the following list of potential threats was compiled from a series of training sessions:

- Escape by one or more prisoners
- Unauthorized entry into the facility
- Unauthorized movement within the facility
- Introduction of contraband into the facility
- Inmate assault on staff
- Inmate assault on another inmate
- Major disturbance or riot
- Inmate suicide or attempt
- External attack on the facility
- Terrorism
- Natural disaster such as a hurricane, tornado, or flood
- "Political" threat[7]

The preceding list should be considered a starting point for the threat definition process. The objective is to describe what is important and of most concern at this time.

Examining data and information may help to identify threats that are the most concern. Facilities involved with the accreditation process are familiar with the need to collect and analyze critical incident data and more recently, the expanding series of "outcome measures" that are integral to the new performance-based standards. These sources offer some additional ideas for threat identification and may also help to assign priority to threats. Some examples of some of those outcome measures follow:

Outcome Measures[8]

- Worker compensation claims filed for injuries
- Illnesses
- Physical injuries
- Vehicle accidents
- Emergencies
- Times that normal facility operations were suspended due to emergencies
- Injuries requiring medical attention that result from emergencies
- Injuries resulting from fires
- Code violations cited in the past 12 months
- Incidents involving toxic or caustic materials
- Incidents of inventory discrepancies
- Other incidents
- Unauthorized inmate absences from the facility
- Instances of unauthorized access to the facility
- Instances in which force was used
- Weapons found in the facility
- Controlled substances found in the facility

[7] While different than the other threats on the list, we have found that many jail operators are concerned about the political dimensions of jail operations. In one facility, employees expressed concern that visitors and volunteers would complain to elected officials if they are "inconvenienced" during their visit to the jail.
[8] F*rom* several Performance-Based Standards books, American Correctional Association, Lanham, Maryland. 2003-2004.

- Incidents involving keys
- Incidents involving tools
- Incidents involving culinary equipment
- Incidents involving medical equipment and sharps
- Incidents in which staff were found to have acted in violation of facility policy
- Staff terminated for conduct violations
- Staff substance abuse tests failed

Data and information about the events that are described in the preceding list could help to identify potential threats *and* determine which threats are of most concern. Examine each of the outcome measures separately. For instance, you may not have had an "unauthorized inmate absence," but there may have been several "incidents involving keys" and "incidents involving culinary equipment."

There are many undesirable events to consider. Tailor your threat definition to your specific needs and priorities.

As you finish your threat definition process, you feel uncomfortable about your facility and operations. After exploring and defining threats for his facility, one training participant exclaimed that he "would never sleep again." The final phase of the JVA process implements an ongoing process that has brought peaceful nights to many jail managers.

Remember, you cannot assess the vulnerability of your facility, technology, and operations without clearly defining the threats that will be challenging them. Define several threats, clearly and concisely. If some are more pressing than others, put the list in order of priority.

Defining Threat *Capabilities*

Now that threats have been described, it is time to determine the *capabilities* that threat participants might bring to bear. Not all threats are equal, and not all threat participants bring the same constellation of capabilities to their tasks.

Threat participants bring a variety of resources, including:

- Knowledge
- Skills
- Abilities

Do not underestimate your adversaries. In one county, an inmate was able to escape through the wall of a jail. It turned out that he had been on the construction crew that renovated the facility for use as a jail and knew exactly what was in the exterior walls and how to exploit its weaknesses. The *knowledge* of the jail's construction was a critical element of his success. Similarly, consider the skills and abilities that threat participants might possess.

Inmate knowledge often includes a working knowledge of jail procedures and practices. Do not fall in to the trap of thinking that "our inmates aren't here long enough to worry about them figuring out our practices." Although many jail inmates are booked and released within a few days, the majority of inmates who take up the jail beds spend months in confinement. And many inmates return to jail many times.

Inmates often bring skills from the community, such as construction or electronics experience. The Pennsylvania Department of Corrections discovered that they had an inmate who had installed exterior sensor systems before he was incarcerated. Some inmates have abilities that may enhance their tactics; an inmate who is a skilled scam artist will be more formidable when using deceit.

One way to be more systematic about threat capabilities is to review information and data describing previous threats that have been attempted or executed. For example, if you are exploring the capabilities associated with an escape threat, the following list of information offers a good starting point.

Institutional Escape History

1. Identify any past incidents and describe the details of the scenario presented by the inmate(s).
2. Details should include a description of inmate tactics, weapons, escape path elements, tools used, transportation, the time of day, and weather.
3. Was the inmate(s) acting in collusion with anyone from the outside and/or staff?
4. Escape attempts may be accomplished by using either one or all of the following methods: deceit, force, and stealth. The analyst should identify which method(s) was used in the attempt.
5. Examine historical data and information using past records and intelligence information.

The availability of contraband, especially weapons or tools, is a factor that may affect threat capabilities. The following list will help you to identify the nature and extent of this threat in your institution:

Contraband History

1. Determine the type of contraband that is being brought into the facility, such as weapons, drugs, money, and electronic devices.
2. Identify the means in which the contraband is being introduced into the facility, such as visitor areas, daily deliveries, and staff.
3. Determine the means in which the contraband is being packaged.
4. Determine the ownership of the contraband and if it is associated with a specific group or activity.
5. Examine historical data and information using past records and intelligence information.

If inmates are participants in your threats, it is important to understand what types of inmates you house. Examining the characteristics of your inmate population will yield insights in to their capabilities.

Inmate Characteristics

1. What does your "average inmate" look like in terms of age, charge(s), race/ethnicity, address (from the area or not), gang affiliation?
2. How long do your inmates stay in your jail? Examine mean length of stay not just average. Determine the percent of inmates on a typical day who will be housed for more then 90 days, 180 days, and one year.
3. Are inmates classified to determine their level of security risk?
4. Are inmates *housed* according to their classification level?
5. Are inmates assigned work in accordance with an effective classification system?

A sample threat capability checklist for inmate escapes is shown below. It describes the range of issues to consider when defining capabilities, such as:

- Type of inmate
- Assistance (and type)
- Weapons
- Tools
- Vehicles
- Visitors
- Staff
- Other inmates
- Violence

As you describe your threat capabilities, remember that inmates and other threat participants may employ various tactics, including:

- Stealth
- Force
- Deceit

An example of an inmate utilizing stealth would be to hide in a garbage can and be taken out of the secure facility. An example of deceit would be an inmate who acquires a staff uniform and walks out the staff exit.

Appendix A provides Threat Capability Checklists. A sample is provided in Figure 2.1.

One capability that many inmates possess is control over an aspect of their confinement or daily activities. Be especially alert to circumstances in which inmates have some measure of control and consider adding this to your list of capabilities. Sometimes we allow inmates to determine where they go and when they go there. Similarly, inmates sometimes affect the timing of certain activities.

At the end of this step, a concise list of priority threats should be completed. For each threat, the corresponding capabilities of threat participants should be described. As the jail facility, technology, and operations are examined in subsequent steps, findings will be "colored" by these threats and their capabilities.

Figure 2.1: Sample Checklist to Define Escape Threat Capabilities

Threat Capabilities Checklist for *Inmate (Escape)*	***Check (√) if included***
Type of Inmate	
Inmate whose classification does *not* allow him/her outside of the security perimeter.	√
Low security classification inmates escaping from outside the perimeter (i.e. the administration building, warehouse, automotive shop, etc…)	
Low security classification inmates escaping from outside the perimeter on community service jobs	
Assistance	
None.	
Assistance from one other inmate.	√
Assistance from more than one other inmate.	√
Passive assistance from outsider	√
Active assistance from outsider (e.g. crash into the prison through the gate, disable perimeter vehicle or perimeter patrol officer, etc...)	
Passive assistance by staff or contractor	
Active assistance by staff or contractor (ignore alarms; leave gate open, erroneous inmate count, etc…)	
Tools, Weapons	
Tools allowed within the facility.	√
Restricted tools illegally introduced on site (e.g. thrown over fence)	
Weapons legally allowed within the facility.	
Restricted weapons illegally introduced on site (e.g. thrown over fence)	
Vehicles	
Inmate using a vehicle to forcibly exit the perimeter.	
Outsider using vehicle to penetrate perimeter.	
Visitors	
Throwing of contraband over the fence into the perimeter	
Contraband swallowed or concealed by inmate	√
Staff	
Collusion with multiple staff	
Inmates (assist in the introduction of contraband)	
Contraband used while outside the perimeter, or swallowed/concealed to cross the perimeter boundary	
Inmate Violence	
Violence toward staff, contractors, other inmates	√
Riots	

B. Step 1B: Analyzing Facilities, Technology, and Operations

Earlier in this document the three elements of security were described:

- Facilities
- Technology
- Operations

In a perfect world, we would all have the ideal combination of:

- A *facility* that was designed for our needs and is flexible enough to change
- Good use of *technology* to enhance operations
- Operations that consistently implement the directives contained in policies and procedures.

Few jails operate in such an ideal situation. This step of the process helps you systematically describe and analyze the jail setting.

B1. Characterizing the Institution

Performing a thorough Jail Vulnerability Assessment requires a clear understanding of the context in which the JVA is being conducted. By "characterizing" the institution you identify building structures, high traffic areas, infrastructure, terrain, weather conditions, historical data, inmate characteristics, and other features that could affect vulnerabilities.

But a description of the institution does not provide needed insights. Rather, the threats defined in the preceding steps are applied against the physical setting to identify deficiencies and concerns.

You may want to take the time to conduct a thorough inventory of physical characteristics, using and annotating various construction documents and plans. Appendix B provides detailed checklists that may be used.

The checklists in Appendix B help you to identify key characteristics of the institution and the broader site and location. You will start by pulling back from the facility and looking at the big picture: location and its implications, such as access to transportation systems. Moving closer, you will examine the site, also identifying features that have implications for safety and security. From there, facility design and construction are examined. Finally, attention is given to technical systems.

These draw your attention to:

B1: Location. This inventory focuses on the location of the facility within the broader context of the neighboring activities and features. It looks at what is located near and nearby the site. We often take our neighborhoods for granted, and we rarely get to choose where our jails are located. Identifying and understanding the context of our location is essential to safety and security. Your team should answer the question "W*hat aspects of the location make my threats more feasible?*"

B2: Site plan. This inventory focuses on the features of the *site* on which the facility is located**.** It helps identify boundary lines, roads, the land uses of adjacent properties, and major topographical features. "*What elements and characteristics of the site may facilitate the success of threats?"*

B3: Facility Design, Layout and Construction**.** This inventory focuses on the characteristics of the facility itself, including the way it is designed, its overall layout, and the types of construction. Beginning from the outside with egress and access point, this checklist will walk you through the way your building was constructed. *"What design, layout and construction features create vulnerabilities to the defined threats?"*

B4: Video Systems. This inventory focuses on the video systems that are used in and around the facility. Beyond that, it guides you to specifically and thoroughly examine camera features, condition and installations. *"What cameras might be involved with the defined threats, what do they see, who is watching them, and how often?"*

B5: Alarm and Sensor Systems**.** This inventory focuses on the alarm and sensor systems that are used in and around the facility. *"What alarm and sensor systems might interface with the defined threats? What areas lack alarms and sensors and thereby increase vulnerability?"*

B6: Metal and Other Detectors. This inventory focuses on the various detectors that are available and are used in the facility. *"What metal and other detectors might be involved in my threat(s)?"*

For each of these inquiries, the checklists prompt you to consider:

- Proximity and Adjacency: For each threat, list features that both benefit and detract from your security because of proximity and adjacency. What features pose a threat because they are *near* or *next to* each other? Conversely, you will also consider situations in which vulnerability is increased because elements are not close together.
- Visibility and Observation: For each of your defined threats, identify areas in which the lack of visibility and poor observation pose a challenge to your security.
    - Identify blind spots, poor lines of sight, obstructions and other features that might pose a threat
    - Consider environmental conditions such as rain, fog, and snow that affect visibility and observation.
    - Think about how visibility and observation change by season, time of day, and even day of the week.

- Do you get a lot of snow in your yard and use inmates to clear it?
- Is there potential flooding nearby?
- Do you increase yard time in the summer because your jail is hot?

- Continuity**:** Identify instances in which continuity of features or systems is interrupted. Adversaries will exploit weaknesses in your facility, technology or operations. If CCTV coverage of the perimeter is strong on three sides of the complex, but is weak in the fourth, adversaries will likely exploit this discontinuity. For each identified threat, describe instances of discontinuity.

- Condition: Identify features with conditions that pose a potential vulnerability, such as sensors that have not been adequately maintained or control panel lights that do not work. A review of your maintenance work orders over the past year would be helpful. For each defined threat, describe features whose conditions increase risk.

What does this step look like in practice? It may take various forms. One of the most successful approaches involves making a series of site visits throughout the jail, focusing on different dimensions each time. The first excursion might focus on proximity, visibility, and observation. The second might focus on continuity and condition. Another strategy divides the JVA team into small groups, assigning one or more perspectives to each.

As you visit all areas of the facility, be sure to record all observations. Some of your findings might not be directly related to your defined threats, but may require attention.

B2. Detection

Remember the three elements of physical protection systems?

- Detection
- Delay
- Response

The next round of inquiries will focus on detection of undesirable activities and events. Appendix M provides a “primer” on physical protection systems, with an emphasis on physical and technical dimensions of detection, delay, and response. Consult the appendix if you would like more technical information.

Appendix C, page C-1 provides a checklist to guide your analysis of detection systems and practices. The checklist describes a series of tasks that will:

- Identify entry controls systems
- Determine the process for key control
- Describe the manner in which packages are processed
- Document procedures that allow access and egress
- Identify and describe perimeter features
- Determine the reliability of systems
- Identify the integration between detection and assessment

- Determine physical and environmental conditions that affect detection
- Examine data and information about past incidents and performance
- Identify video systems and capabilities
- Observe officer stations and posts
- Identify activities and events that might distract officers

In addition to using the checklist, your inquiries must consider the four perspectives that were introduced in the previous step:

- Proximity and Adjacency
- Visibility and Observation
- Continuity
- Condition

Participants in the JVA process should spend ample time in and around the facility using the checklist as a tool and focusing on the four perspectives. Findings should be accurately recorded for later analysis.

B3. Delay

The next round of inquiries will focus on elements that present "delays" to your identified threats. Appendix M describes delay systems and features in detail.

The checklist on Page C-2 of Appendix C provides guidance, including attention to:

- Perimeter delay features such as fences, gates, and in many jails, the building itself
- Vehicle barriers
- Construction of walls, windows, doors, roofs, and floors
- Instances in which detection is not triggered before delay
- Multiple layers of delay, or "protection in depth."

In addition to using the checklist, inquiries should consider the recurring four perspectives:

- Proximity and Adjacency
- Visibility and Observation
- Continuity
- Condition

Again, the team should spend ample time in and around the facility, using the checklist as a tool and focusing on the four perspectives. Findings should be accurately recorded for later analysis.

B4. Response

This step explores the third element of physical protection systems—response. The checklist on Page C-3 of Appendix C lists of series of items that should be examined, including:

- Types of communication available to officers and backups

- Internal communications systems for major events
- Operator ability to assess activity
- Response timeline (how long it takes after detection)
- Type of response force
- Number and type of primary responders
- Post and patrol locations
- Response force training
- Ability to monitor diversionary tactics

In addition to using the checklist, inquiries should consider the recurring four perspectives:

- Proximity and Adjacency
- Visibility and Observation
- Continuity
- Condition

The team should spend sufficient time in and around the facility, using the checklist as a tool and focusing on the four perspectives. Findings should be accurately recorded for later analysis.

B5. Operations

The final task in this series focuses on actual daily operations. At this point, you have identified threats as well as threat capabilities.

Policies and procedures are the cornerstone for jail operations. They describe, in advance, what everyone is *expected* to do in hundreds of situations. Policies and procedures provide the basis for post orders, and are central to all staff training activities.

In the final analysis, policies and procedures signal our *intentions*, but do not necessarily reflect what actually happens from day to day. Examining operations provides an honest and objective comparison of what is supposed to happen (policy and procedures) to what actually happens (practices).

Maintaining security is a continuous process. It demands the efforts of sufficient numbers of staff who are:

- Qualified
- Properly trained
- Directed by policies and procedures
- Supervised to ensure that the practices match the policies and procedures
- Properly deployed (in the right place, at the right time)

When we come up short on any of the above components, security suffers and we open ourselves up for adverse events.

Appendix D offers resources that will help you to systematically examine your current practices. The exhaustive set of protocols and practices provided in Appendix D portrays sound practices, as defined by experts in the field.

Section II is the centerpiece of Appendix D, providing specific recommended practices that address each of the following topics:

A. Operations
- A1. Staffing
- A2. Inmate accountability
- A3. Emergency preparedness
- A4. Intelligence
- A5. Searches
- A6. Institution visiting
- A7. Transportation of inmates (escorted trips)
- A8. Security inspections
- A9. Training

B. Equipment and technical systems
- B1. Video systems
- B2. Alarm and sensor systems
- B3. Metal and other detectors
- B4. Physical plant security
- B5. Perimeter security
- B6. Locking systems (key/lock control)
- B7. Control center
- B8. Tool control
- B9. Utilities and mechanical systems
- B10. Toxic/caustics control

C. Physical plant
- C1. Location and site
- C2. Building layout and construction
- C3. Entrances and exits in the secure perimeter
- C4. Armory
- C5. Mail room
- C6. Trash collection/disposal

Operational characteristics are also addressed in Appendix B. Checklist B7 outlines the breadth and depth of inquiry, including:

1. Manpower surveys, staffing patterns, and schedules
2. Historical reports (past/present/future)
3. Site detection/delay/assessment systems
4. Weapons/emergency equipment inventory
5. Operational procedures
6. Policy requirements
7. Overall inmate classification scores/patterns
8. Jail crowding measures – design capacity versus actual population numbers
9. Performance test data, (tests conducted on systems e.g. backup generator)
10. Security inspection results

The final round of site visits will focus on the practices that occur in the facility. If adequate time is allocated, team members will be able to observe employees, inmates, contractors and others as they go about their daily routines.

Participants should have enough time to stay in an area until operations return to normal and are not skewed by their presence.

In addition to using the checklist in Appendix B, on site inquiries should consider the four perspectives in the context of operations:

- Proximity and Adjacency
- Visibility and Observation
- Continuity
- Condition

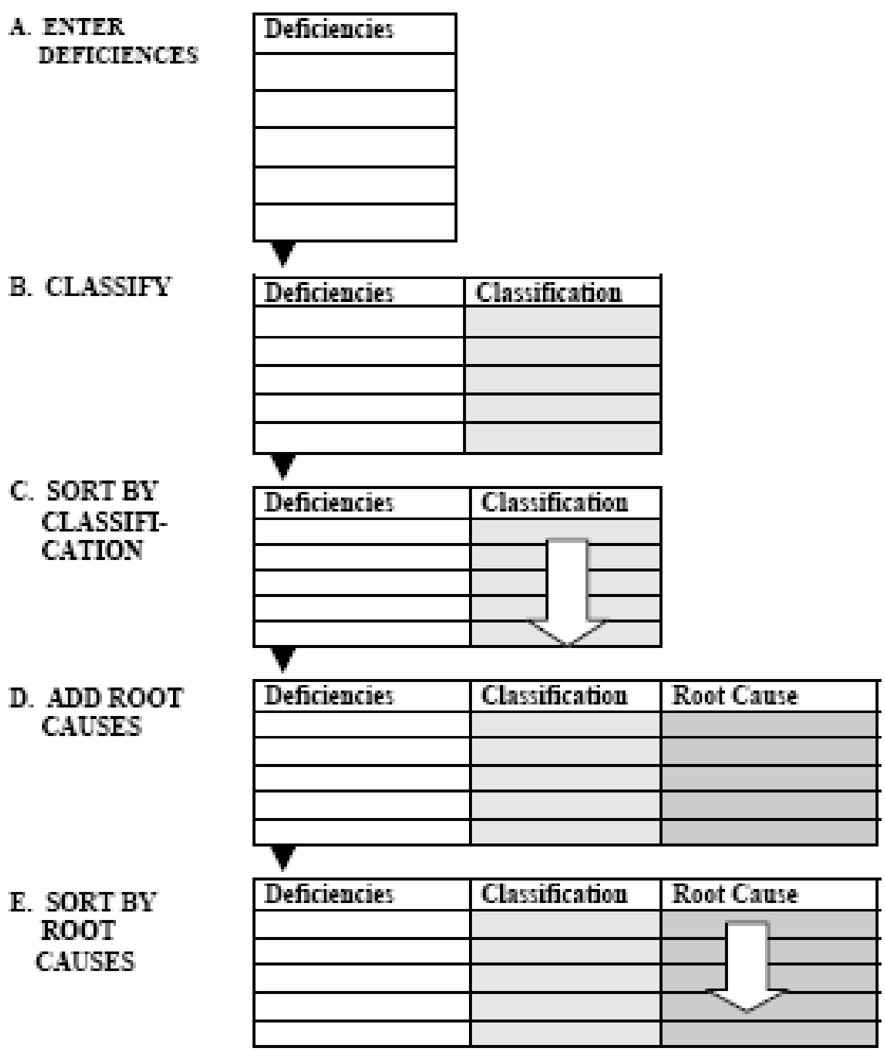
Findings should be accurately recorded for later analysis.

C. Step 1C: Assembling and Classifying Findings

At this point in the process, many deficiencies and concerns have been identified. The initial lists of deficiencies may look daunting, both in length and breadth. The deficiencies are mixed and need to be processed as a starting point for analysis.

Figure 2.2 describes the overall process that is used to assemble, classify, and identify “root causes.” The first four steps in the process will be implemented before Phase One is completed.

Figure 2.2: Steps in Processing Findings



Collect All Findings (A)

Step A on the process diagram requires assembling all findings into a single list. It is best to make a one-column table for the list, as it will provide a format that makes subsequent steps easier. Figure 2.3 shows the relevant excerpts from the diagram.

Figure 2.3: Assembling Findings in a Table

Deficiencies

A sample of findings has been drawn from experience in the field. These few findings provide a cross section of deficiencies, and will be used to demonstrate the process in subsequent steps.

Figure 2.4: Sample of Findings Assembled in a Table

A. Deficiencies

DEFICIENCIES
Leaving gate open allows piggybacking, contraband, escape, etc
Storage room not monitored with camera
Kitchen utensils left unattended
No security officer in kitchen
Door to holding areas equipped with electric lock, but is currently propped open.
Lock on exterior door doesn’t latch
Height of booking desk area not adequate to prevent inmate access
Dangerous utensils (scissors) in direct line of sight of inmates
Drain grate in floor of holding cells have sharp or missing pieces

Classify Each Finding (B)

Adding a column to the right of the table provides space to describe a primary classification for each finding. There are three categories, reflecting the three components of safety and security:

1. Facilities
2. Technology
3. Operations

Figure 2.5 shows the structure of the table for this step, and Figure 2.6 carries the sample into the next format.

Figure 2.5: Classifying Each Deficiency

Deficiencies	Classification

Figure 2.6: Sample of Classification

B. Classify

DEFICIENCIES	CLASSIFICATION
Leaving gate open allows piggybacking, contraband, escape, etc	Operations
Storage room not monitored with camera	Technology
Kitchen utensils left unattended	Operations
No security officer in kitchen	Operations
Door to holding areas equipped with electric lock, but is currently propped open.	Operations
Lock on exterior door doesn’t latch	Facility
Height of booking desk area not adequate to prevent inmate access	Facility
Dangerous utensils (scissors) in direct line of sight of inmates	Operations
Drain grate in floor of holding cells have sharp or missing pieces	Facility

Sort by Classification (C)

After each deficiency has been assigned a single primary classification, sort the table by classification.

Figure 2.7: Sorting By Classification

Deficiencies	Classification

The sample, sorted by classification, is shown in Figure 2.8.

Figure 2.8: Sample Sorted by Classification

C. Sorted by Classification

DEFICIENCIES	CLASSIFICATION
Lock on exterior door doesn’t latch	Facility
Height of booking desk area not adequate to prevent inmate access	Facility
Drain grate in floor of holding cells have sharp or missing pieces	Facility
Leaving gate open allows piggybacking, contraband, escape, etc	Operations
Kitchen utensils left unattended	Operations
No security officer in kitchen	Operations
Door to holding areas equipped with electric lock, but is currently propped open.	Operations
Dangerous utensils (scissors) in direct line of sight of inmates	Operations
Storage room not monitored with camera	Technology

This initial sorting helps to cluster the findings by type. This makes the next step (root causes) easier.

Identifying Root Causes (D)

A third column is now added to the table. For each deficiency, determine the "root cause" that causes the deficiency. Think of deficiencies as symptoms, and root causes as the condition that creates the symptom. Sometimes there will be more than one root cause for a deficiency.

Figure 2.9: Identifying Root Causes

Deficiencies	Classification	Root Cause

The sample in Figure 2.10 identifies several distinct root causes.

Figure 2.10: Sample of Root Causes

D. Root Cause Added

DEFICIENCIES	CLASSIFICATION	ROOT CAUSE
Lock on exterior door doesn't latch	Facility	Maintenance
Height of booking desk area not adequate to prevent inmate access	Facility	Design
Drain grate in floor of holding cells have sharp or missing pieces	Facility	Maintenance
Leaving gate open allows piggybacking, contraband, escape, etc	Operations	Supervision
Kitchen utensils left unattended	Operations	Supervision Training
No security officer in kitchen	Operations	Staffing
Door to holding areas equipped with electric lock, but is currently propped open.	Operations	Training Supervision
Dangerous utensils (scissors) in direct line of sight of inmates	Operations	Policies/Procedures
Storage room not monitored with camera	Technology	Funding

Why identify root causes? Because it assembles the deficiencies into a relatively small number of groups that have solutions in common. Using this approach, a manageable number of causes emerges. Root causes also make it easier to develop solutions because they already point toward the source of the problem.

The final step in the sorting process involves sorting the table by root cause (primary sort key) and classification (secondary sort key). If a deficiency has more than one root causes, which is sometimes the case, a separate row will need to be made for each root cause, as shown in the sample.

Figure 2.11: Sorting by Root Cause (E)

Deficiencies	Classification	Root Cause

Figure 2.12: Sample Sorted by Root Causes

E. Sorted by Root Cause and then classification

DEFICIENCIES	CLASSIFICATION	ROOT CAUSE
Height of booking desk area not adequate to prevent inmate access	Facility	Design
Storage room not monitored with camera	Technology	Funding
Lock on exterior door doesn't latch	Facility	Maintenance
Drain grate in floor of holding cells have sharp or missing pieces	Facility	
Dangerous utensils (scissors) in direct line of sight of inmates	Operations	Policies/Procedures
No security officer in kitchen	Operations	Staffing
Leaving gate open allows piggybacking, contraband, escape, etc	Operations	Supervision
Kitchen utensils left unattended	Operations	
Door to holding areas equipped with electric lock, but is currently propped open.	Operations	
Kitchen utensils left unattended	Operations	Training
Door to holding areas equipment with Electric Lock, but is currently Propped open.	Operations	

Each facility will generate a unique breadth and mix of root causes. At a training session, participants reported the following root causes generated during their field exercises.

Figure 2.13: Sample Root Causes

- Activity scheduling (plan of the day)
- Classification
- Controlled by others (agency did not have authority)
- Crowding
- Employee schedules
- Employee selection and retention
- Employee supervision
- Equipment
- Facility construction
- Facility design
- Inmate supervision
- Maintenance
- Policies and procedures
- Staffing
- Technology
- Training

The following list elaborates on some of these root causes and suggests additional ones:

- Inappropriate *policies* (setting out to do the wrong thing)
- Inadequate *procedures* (not attempting to do it the right way)
- Training *deficiencies* (not arming staff with the knowledge, skills and abilities they need)
- *Employee supervision* (employees actions not corrected and reinforced by first line supervisors)
- *Staffing* issues (insufficient staff, wrong type of staff assigned, inadequate deployment, etc.)
- *Equipment* shortcomings (the wrong equipment for the application, poor installation, failure to maintain the equipment, etc.)
- *Physical plant* problems (poor design, construction, inadequate maintenance, etc.)

Sometimes it is helpful to ask “why” in the quest for root causes. For example, employees fail to lock a holding cell door when it is occupied. Why? Were they not directed to lock the cell by policies and procedures? Were procedures sufficient, but training failed to deliver the message? Or was the training sufficient, but not reinforced by effective first line supervision?

This approach to identifying root causes proves productive. The root cause analysis sets the stage for identifying solutions in Phase Three.

CHAPTER 3: Phase Two- Advanced Risk Identification

NOTE: You may decide to begin working on solutions to the problems identified in Phase One, concurrent with starting Phase Two.

Introduction

The first phase of the JVA process identified many problems and concerns. Most of these were freestanding issues, such as a lock that malfunctions, or a blind spot in a camera's viewing area. Such ad hoc concerns are found throughout the facility and its surrounding area. Each, by itself, poses a potential risk when compared to the identified threats and their capabilities.

This second phase of the JVA process employs methods and tools that were developed by Sandia National Laboratories. These provide an advanced level of scrutiny, but also build on the work done in Phase One. The Phase Two activities:

- Turn observations from Phase One (anecdotes) into *data* (probabilities of detection, delay times, and response times)
- *Connect* elements of the physical protection system (facilities, technology, and operations)
- Identify series of *steps* (pathways) that might be used to execute a threat
- Put the elements in *motion* by measuring times associated with each step in the pathway
- Determine the probability of *detection* for each step
- Calculate the statistical *probability* that the threat will be neutralized before the steps are completed

This "advanced" level of analysis builds on the Phase One findings, but also generates compelling analyses of threat scenarios that underscore the importance of each step in the process (the ad hoc elements identified in Phase One).

This process focuses on the three major components of a physical protection system (PPS) that were explored in Phase One:

- Detection
- Delay
- Response

The steps in this methodology are:

1. Analyzing PPS and operations
2. Developing Path Sequence Diagrams (PSD)
3. Using the EASI model to assess risk

Figure 3.1 describes these steps in more detail.

Figure 3.1: Phase Two Steps

1. *ANALYZE PPS* and Operations ↓	Collecting data and analyzing facilities and operations
2. *CREATE* Past Sequence Diagrams (PSD) ↓	Determining how a series of steps might allow the threat(s) to succeed
3. *APPLY* the EASI Model to Assess Risk ↓	Using the Excel-based tool to predict the likelihood of success

In more simplified terms, the process might be described as judging a race between the facility and the threat. To determine who wins the race, it is necessary to:

- Understand the institutional protection system (physical and operational)
- Determine what the threat can and must do to succeed
- Compare the institution protection system with the threat's actions
- See who wins – look at the timeline

Figure 3.2 is drawn from the Estimate of Adversarial Sequence Interruption (EASI) program, which calculates and draws the timeline and determines how many times the adversary (such as an inmate) will prevail. Step 2B describes how the EASI program is used and Appendix K provides a more detailed explanation including diagrams of the various EASI screens.

In the example in Figure 3.2, time passes after the inmate begins an escape process before the first alarm is sounded. More time passes until the alarm is assessed and response actions are triggered. The response takes less time than the remaining tasks for the inmate, and the inmate is interrupted in his attempt.

Various characteristics of the facility, its use of technology, and operations, conspire to "delay the inmate" as he follows the path of tasks that would lead to an escape.

Figure 3.2 presents a sample time line for an inmate escape scenario. The inmate's actions are shown on the top line, and begin before the first alarm is triggered. The institutional response is shown in terms of the detection, delay and response components. In this sample, the inmate is interrupted before the escape scenario has been completed.

Figure 3.2: Sample Time Line: Inmate Interrupted for Escape is Complete

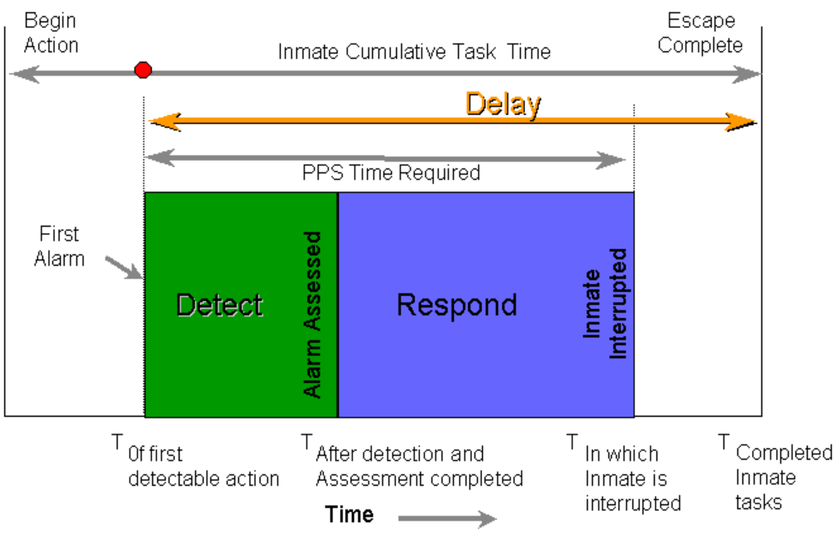
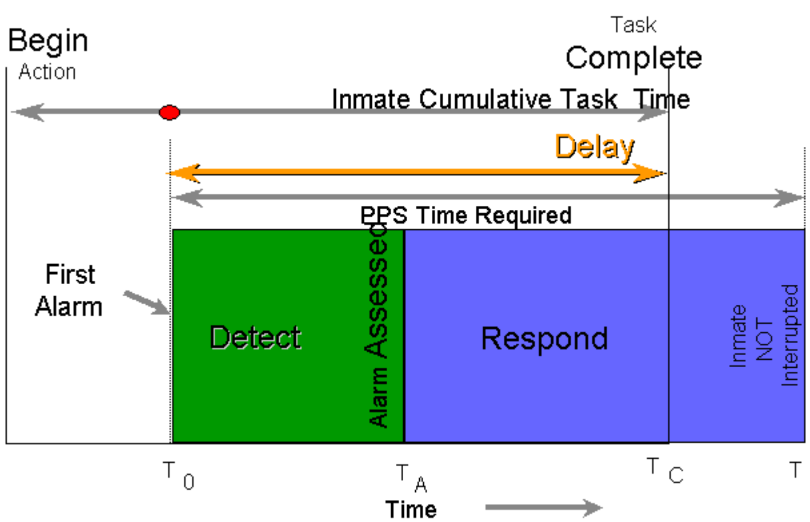


Figure 3.3 shows a time line in which the response comes too late and the inmate is able to escape.

Figure 3.3: Sample Time Line: Inmate Completes Escape



Performance Testing

Phase One underscored the importance of critically examining all aspects of the jail from the perspective of *performance*: what actually happens. Phase Two takes the performance concept further by actually testing performance and collecting data from the tests.

Focusing on performance:

- Determines how each element *really* performs, not what it says on the box or what the vendor told us (performance-based, not feature-based)
- Examines:
    - Threat capability
    - Performance objectives
    - Evaluates effectiveness
- Enables better decisions by:
    - Understanding the system's effectiveness against specific actions
    - Effectively allocating resources

The performance approach also identifies operator failures. For example, a system or an element of a system is functioning properly but procedures are not followed (or are misguided) and the result is failure. Note: many of these problems were identified in Phase One. The performance approach will also identify failures caused by properly conceived and executed procedures that are not integrated.

Appendix M provides a "primer" on physical protection systems. Readers are encouraged to review the appendix, as needed, to supplement their understanding of the technical aspects of security systems and components.

Response

Response is the final component of physical protection systems (PPS). It comes into play in Phase Two. "Response" describes the activities that take place after an undesirable action is detected, in an effort to neutralize the threat.

The "response" checklist in Appendix C identifies the key elements of response:

- The type of communication available to staff and backup types communication
- Internal communication system for major events (i.e. sirens, duress alarms, public address systems) are timely and accurate
- Operator's ability to assess activity, i.e. ergonomics, accessibility to equipment, space availability
- Establish response timeline in accordance with the threats
- Type of response force plans/training (physical and tactical)/performance tested/ratio of officers to inmates
- Number and type of primary responders for a given threat and the number of secondary responders should the need arise
- Post and patrol locations and responsibilities in locating / verifying / isolating / containing / evacuating / resolving / de-activating situations
- Compensatory measures that are implemented when the False Alarm Rate (FAR) or Nuisance Alarm Rate (NAR) are excessively high
- Response force armed vs. unarmed, training and checkout procedures. Equipment appropriate for the assigned task

- Officers’ ability to monitor diversionary tactics, and identify policies in places that address these tactics

Data Collection

It will be necessary to collect data to quantify response times for specific situations that are elements of the scenarios before using the EASI program. Up to this point in the process, findings have been in the form of observations. These are useful and are sufficient in many instances, but sometimes research is required to turn observations into reliable and accurate data. Figure 3.4 describes the differences between observations and data for situations that involve detection, delay, and response.

Figure 3.4: Comparing Observations to Data

Observations (Phase 1)	**Data (Phase 2)**
Officers do not always turn the hand held metal detector on before using it. (Detection) (Operations)	Of 30 times that the hand held metal detector was used, it was not turned on 7 times (23.3% of the times).
The inner control center door is sometimes propped open instead of being secured. (Delay) (Operations)	5 times out of 15 the door was propped open (33.3%).
Officers do not always conduct a thorough search of professional visitors’ brief cases. (Detection) (Operations)	Contraband was not detected in brief cases 3 times out of 12 tests that were conducted (25.0%).
The lock on cell door B-25 does not always latch. (Delay) (Facilities)	The lock failed to latch 6 times out of 28 tests that were conducted (21.4%)
The control room officer does not look at the camera scene for the employee entrance very often. (Detection) (Operations)	An unauthorized civilian was seen by the control room officer 2 times out of 18 tests that were conducted (11.1%).
A movement officer is rarely available to respond to an incident in the outdoor exercise yard. (Response) (Operations)	On 2 out of 14 occasions, a movement officer was available to respond when the outdoor yard was being used. (14.3%)
The image quality for camera A-4 at the staff entrance is poor, making it difficult to identify persons asking to be admitted. (Detection) (Technology)	Unauthorized persons were allowed entry by the control center 7 times, out of 8 times entry was requested, when the control officer was looking at the monitor image from camera A-4. (87.5%)

The data collection forms in Appendix F provide a format for collecting information about entry controls and delays.

There are several ways to collect data, including:

- Field surveys
- Subject matter expert interviews
- Published data (usually provided by the manufacturer of equipment)
- Performance tests

Although published data provided by the manufacturer is the easiest to obtain, it is often the least reliable. It's important to test each system yourself, several times, to ensure that it has been properly installed and maintained and that it is properly operated.

There are other valuable sources of published data. The Department of Defense has published the results of many tests. Sandia National Labs also publishes some of its findings. Appendix G presents some of this data and identifies specific sources for additional data.

There are two basic types of performance tests:

1. Operability test - confirms that a system element or total system is operating
2. Effectiveness test - confirms that a system element or total system is operating as intended or required

If someone walks through a metal detector and an alarm sounds, the detector is considered *operable.* But by taking a piece of metal through the detector at different walking speeds, in different locations on a person's body, helps determine if the equipment is *effective.*

The more tests that are performed, the more reliable the findings. Tests should be conducted at random, at different times and in different locations. Testing is a crucial element that affects the value of the overall credibility of the vulnerability assessment.

Performance test *methods* include <u>limited scope</u> performance tests and <u>full system</u> exercise tests.

The quality of these tests will depend on:

- Detailed planning
- Comprehensiveness
- Conditions
- Recording of results

It is important to *plan* performance tests. Before attempting to test systems and operations you must have a clear plan that addresses safety and security issues.

<u>Caution!</u> The safety of the JVA team and the security of the facility are paramount. Develop specific scenarios for each test, anticipating the circumstances that will be faced and the critical issues associated with testing. One of the issues will be how to handle inmate observation of your activities. Data collection forms should also be developed.

Some tests need to be conducted under a variety of conditions, including:

- Varying weather (fog, ice, snow, extreme heat, blowing sand, etc.)
- Emergency situations
- Different days of the week
- Different shifts

Detection and assessment testing should determine the likelihood of detection for each of the technological sensors. The tests should look for dead spots and use common defeat methods. Tests should determine the effectiveness of personnel in detecting and assessing undesired situations. Tests should be conducted under various working conditions and should simulate situations as many times as possible to produce accurate findings.

Response force data/testing measures the time it takes for the institution to react to an identified problem or situation. These tests not only provide a time line, but also identify the steps involved with the response and the physical/technical elements involved. Response force testing will:

- Determine the time required to use the type of communication available to staff
- Determine the timeliness of internal communication systems for major events (sirens, duress alarms, public address systems)
- Verify the number and type of primary and secondary responders
- Include diversionary tactics
- Test all significant elements of the response timeline

It is imperative to accurately and completely record all test results.

Poor recording may:

- Invalidate the test
- Cause additional testing
- Portray a false image

There are three basic ways to analyze test results:

- Statistical analysis
- Validated expert judgment
- Expert judgment

Accurate and reliable data are essential to ensure that the EASI findings will be credible. It is not sufficient to estimate a probability of detention or the number of seconds of delay. Rather, testing, or when that is not possible, other reliable methods must be employed.

A. Step 2A: Path Sequence Diagrams (PSD) and Scenarios

"Path Sequence Diagram" (PSD) is a fancy name for a map that shows how an inmate, employee, contractor, or other person might navigate through the facility to affect a threat. A PSD might also show how someone might introduce contraband or how any number of other defined threats might be implemented.

Path sequence diagrams:

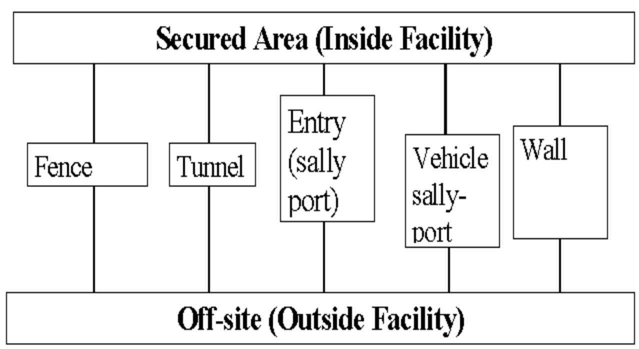
- Provide a graphical model used to help understand the PPS at a facility

- Depict:
  - Paths that inmates can follow
  - PPS elements along the paths

- Assist the JVA team to determine the most vulnerable path(s)

Figure 3.5 depicts a simple PSD.

Figure 3.5: Simple Path Sequence Diagram



The PSD in Figure 3.5 (above) shows the physical elements that exist between an inmate who is inside the facility, and freedom outside the facility.

Figure 3.6 provides a more complex PSD, indicating the path that might be chosen by an inmate to move successfully from a cell to an area outside of the security perimeter. The arrows in the center of the PSD show points at which alarms are raised, and where those alarms are communicated.

Figure 3.6 shows the path of least resistance or the path that offers the best chance for success for the inmate. Rather than attempting to exit from the cell by a window, wall, or mechanical chase, the inmate selects the door. There are similar choices at each point in the diagram, although this simplified version does not depict them. Alarms are indicated by arrows which show where the alarms are sounded.

Figure 3.6: Path Sequence Diagram

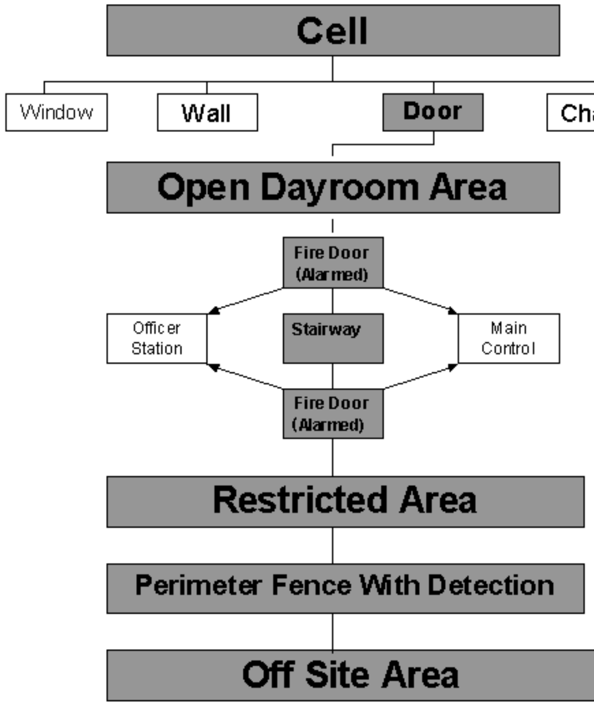
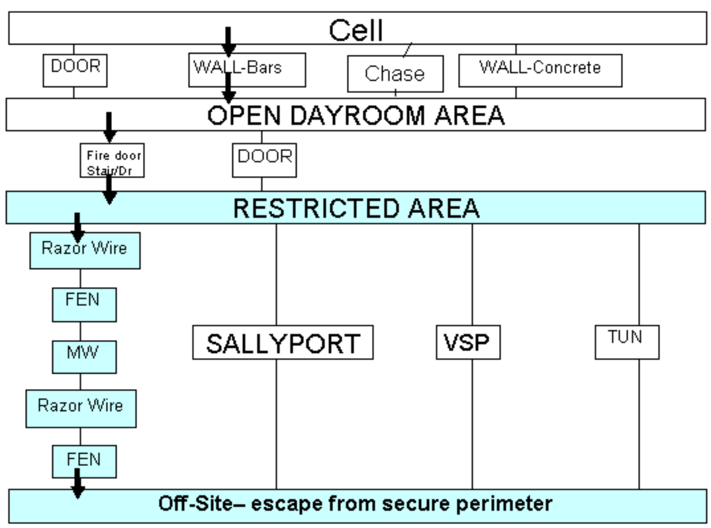


Figure 3.7 shows the larger context from which one or more PSDs are identified. Note that there are multiple choices to move from the cell block and the open area. This type of larger diagram, from which PSDs are identified, is sometimes called an "Adversary Sequence Diagram" (ASD).

Figure 3.7: Sample Adversary Sequence Diagram (ASD)



To construct a path sequence diagram for a threat of inmate escape:

1. *Begin where the inmate could start an escape. Consider a simple diagram or a list to show the places the inmate could start, such as:*
    a. *Cell*
    b. *Kitchen*
    c. *Recreation yard*

2. *Identify all the ways the inmate could leave the first area. Be sure to look up and down as well as side to side.*

3. *Go to the area outside the first one and identify all the ways the inmate could leave the new area*

4. *Continue this until the inmate is outside the facility*

When selecting starting points, consider the places that inmates usually occupy, such as housing units, work sites, program/medical areas, and such. Also be alert to any opportunities that inmates might have to control events and the timing of events. For example, the inmate who does housekeeping duties for a housing unit might have the ability to control or affect when garbage is removed.

At this early stage of the analysis, be sure to identify *all* of the ways that an inmate could move from one space to another, no matter how futile they might seem. It is important to draw the full picture so that the decisions that the inmate might make are put in context.

Write the following on each PSD drawing:

- Time of day
- Day of week
- Conditions
- Tools/aids assumed available to inmate (capabilities)

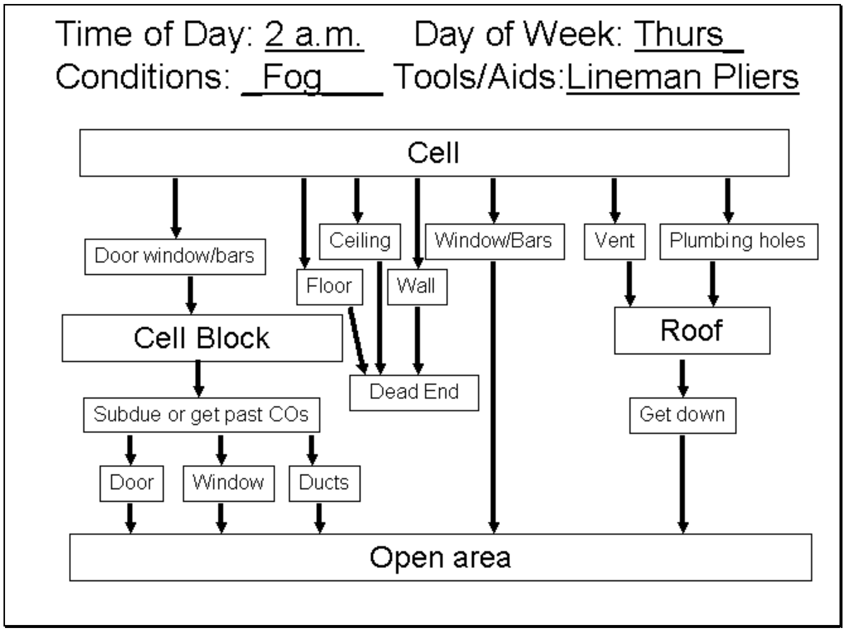
Appendix H provides a tool to help you create your path sequence diagrams. The PSD Checklist in Appendix H identifies all of the elements in each space, and how to record them properly.

Figure 3.8 provides a sample of a working PSD document. Note that the time, day of week, tools/aids and conditions are filled in.

There are several paths that lead to a "dead end" on Figure 3.8. There are times when it is simply not possible for a path to continue, under the threat conditions you have defined. When these are encountered, it is appropriate to indicate that a dead end has been reached.

Be careful not to be too hasty in reaching this conclusion though, and be sure to seek the advice of your fellow JVA team members before eliminating any avenue. When a decision is made to eliminate a path or an element as a dead end, be sure to document the reasons. It is important to have a clear and concise record of activities and conclusions. Diagrams that have dead ends will prove that *all* of the potential paths and options have been considered.

Figure 3.8: Sample Worksheet for PSD



It is important to revisit each PSD under different times, days, conditions, and assumptions (e.g. tools, weapons). A path that might be readily detectable from an officer's post in daylight might offer a new range of opportunities after dark. Posts that are staffed on weekdays might not be activated on weekends. There are many variations to consider, and adversaries often have lots of time to process all of them, and to look at all the angles.

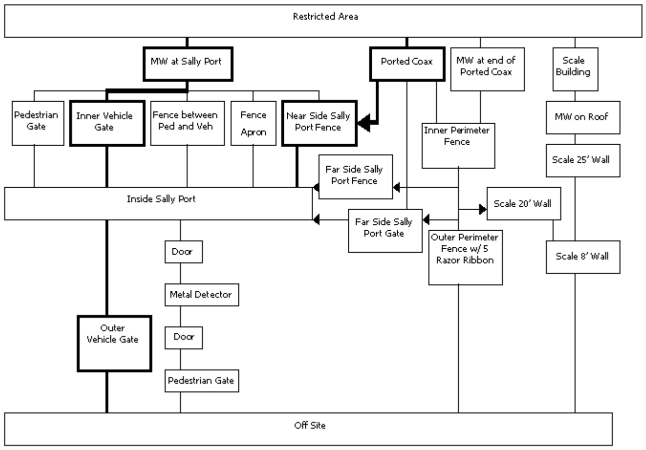
Figure 3.9 presents a PSD for a typical perimeter. The PSD in Figure 3.9 indicates two paths from the restricted area that converge at the inside sally port. From there, both follow the same path out of the facility.

It will be tempting to identify only the path of "least resistance." But this path often has the highest potential for detection. Some paths might involve more time or difficulty overcoming barriers, but also avoid detection longer. In other words, threats will often choose to confront a longer delay instead of facing a higher probability of detection.

At this point in the process, a great deal of information, data and insight has been assembled. Nothing has been *discarded*. In the next step, attention will be focused on the most serious and viable threats.

Caution! **Do** not **lose anything that you have assembled or identified** up to this point in the process. As PSDs are discarded, be sure to keep them as part of the record for the JVA. Most importantly, be sure to keep a running list of specific questions, concerns, and problems that have been identified, whether they are connected to an active PSD or not. In this way, you continue to add to the growing list of issues that was started in Phase One.

Figure 3.9: Sample Perimeter Path Sequence Diagram (PSD)



Developing Scenarios

The term "scenario" describes writing a script for a series of actions. The dictionary defines a scenario as a "hypothesized chain of events" which fits the use of the term in the jail vulnerability assessment process.

Having created a number of path sequence diagrams up to this point in the process, it is time to take each one out in turn and examine it.

The steps for developing scenarios are:

a. Look at each PSD and identify how to defeat each of the security elements.

b. Select the most reasonable defeat or bypass techniques for each of the elements.

c. Estimate the "probability of detection" ($P_{D)}$ and delay times for each element for each defeat technique.

d. Record this information on the PSD.

e. Evaluate the PSD for paths that have low detection.

f. Identify paths that have low delay times.

g. Select a few scenarios for more detailed evaluation.

To accomplish this task, you may have to collect the information by consulting facility construction documents, equipment operating manuals, incident data, and other sources.

a. Look at each PSD and identify how to defeat each of the security elements.

Threat definition and capabilities were explored in Phase One. Remember that inmates and other threat participants have a variety of tactics that may be employed, including:

- Stealth (such as sneaking)
- Force
- Deceit (such as wearing a uniform, forging a pass)

Be sure not to discount the capabilities of the inmates and other threat participants:

- Knowledge
- Motivation
- Skills
- Abilities

There are many ways that inmates "defeat" us in the correctional setting, including:

- Deceit
- Collusion
- Stealth
- Force
- Knowledge
- Information/intelligence (inmates sell information about the facility to each other)
- Tenure (many inmates have been at the facility longer than the staff members)
- Train us (inmates are sometimes able to *alter* staff behavior over time)

Here is an example of how various tactics might be employed by an inmate:

Cell Example

- Officer opens the cell and is overpowered by inmate (force), or
- Inmate sneaks past officer (stealth), or
- Inmate gets keys and opens the door by appearing authorized to open the door (deceit), or
- Inmate sneaks up on officer and takes the keys (stealth), or
- Inmate just takes the keys from the officer (force)

b. Select the most reasonable defeat or bypass techniques for each of the elements.

Select the most reasonable method to either defeat or bypass the element. The decision might be based on either which is the easiest method, or which is most likely to avoid detection, or a combination of the two.

To make these decisions, you will need to list the features at each element for each path. Figure 3.10 provides an example of how the features might be described.

Figure 3.10: Sample List of Features for Inmate Cell

Inmate Cell Example

- Wall -12" thick concrete wall with rebar at 6" centers, 4" diameter sewer and water hole, 6"x12" vent with 1/8" grating
- Cell door - two 1/4" steel plates
- Electronic lock
- Open cell door sensor
- 3"x12" Window with one bar
- Personnel generally in vicinity
- Random bed checks by correctional officers

Record the chosen defeat or bypass technique next to each element on the path sequence diagram (PSD).

c. Define probability of detection (P_D) and delay times for each element for each defeat technique.

Where can information needed to define P_D or estimate delay times be found? Figure 3.11 suggests the three primary sources, including:

- Observations from touring and examining the facility
- Institution documents
- Testing data
- Printed data
- Expert opinion

Figure 3.11: Sources for Obtaining Detection Probabilities

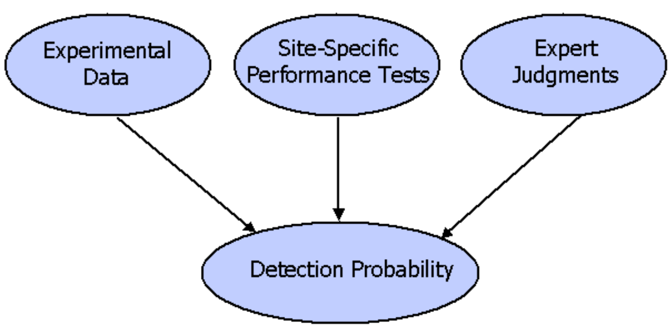


Figure 3.12 provides an example of information that might be derived from testing. The results shown in Figure 3.12 are from testing conducted at Sandia National Laboratories. It is important that you develop local data to ensure its applicability to your facility.

Remember that the data being collected is not *whether* an element can be defeated, but rather how long it takes and how likely it is that the effort will be detected.

Figure 3.12: Example of Data from Testing

Event	**P_D**	**Delay Time**
Metal core door		12 seconds delay per door
Climb 14 ft fence		20 second (climbing)
Microwave exterior detection system	0.9 probability of detection	
30-cm, reinforced concrete		170 seconds
Tilt/vibration fence sensor	0.8 probability of detection	
1.6-mm doors (one door into controlled building area and one outside door)		60 seconds
Officer at post	0.5 probability of detection	
Officer at post		30 seconds
Microwave exterior detection system	0.9 probability of detection	
Detectors on building doors	0.99 probability of detection	
Interior detector	0.9 probability of detection when on	
Average officer response time		60 seconds

The decision-making model for the JVA process is *consensus.* As each element is examined and decisions are made regarding detection, delay, and ultimately whether to discard a path, it is important for all team members to concur.

d. Record Information on PSD

Recording the data detection and delay next to each element on the PSD makes it easier for the team to analyze the relative feasibility of each path, as shown in Figure 3.13.

Figure 3.13: Detection and Delay Recorded on PSD
(Detection record as decimal, delay in seconds)

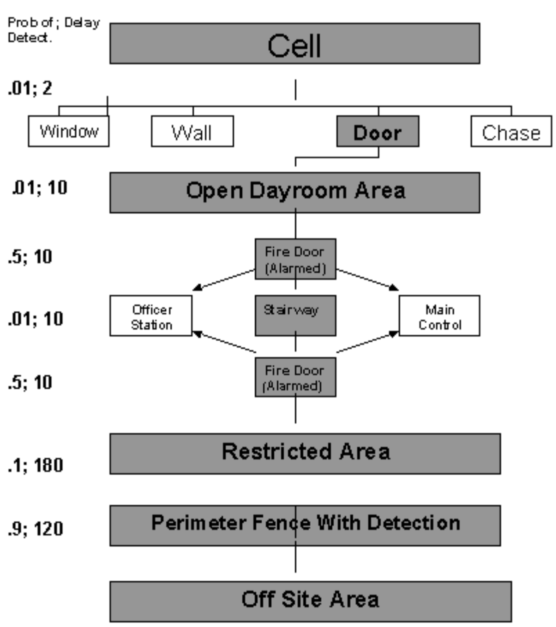
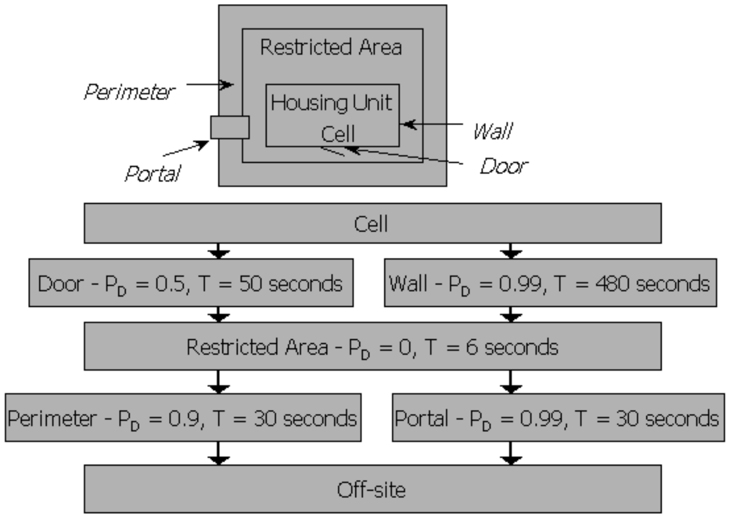


Figure 3.14 provides another format for recording PSD and corresponding values.

Figure 3.14: PSD with Detection and Delay Values



e. Evaluate the PSD for paths that have low *detection*.

The next task is to look at the PSD to identify paths that present a low level of detection. Figure 3.13 suggests that the first two steps in the path have an extremely low detection probability (.01, or 1 percent). The alarmed fire doors (steps 3 and 5) have a 50/50 chance of detection, and the probability for the final step--the fence-- is 90 percent.

At first glance, it is likely that the inmate will be detected by the time he/she emerges from the second fire door. Examine other PSDs and find those that have the overall lowest likelihood of detection and put them aside for further review.

f. Evaluate the PSD for paths that have low *delay times.*

As with the previous task, look at *all* of the PSDs in terms of delay times. Remember, this is a race between the threat and the facility. The longer it takes the threat to complete each step of the path, the more time the facility has to detect, assess and respond.

Looking at Figure 3.13 again, the delays are relatively short in the first five steps (a total of 42 seconds.) The path slows considerably at the sixth step (3 minutes), which could be crucial time if the inmate has been detected coming through the fire doors. Another two minutes are required to negotiate the final step.

g. Select a few scenarios for more detailed evaluation.

Now it is time to narrow the field of vision and focus on a few specific scenarios. The scenarios have already been sketched out through previous efforts to identify the defeat or bypass techniques (describe what the threat will do), calculate the likelihood of detection for each element (or step in the scenario), and estimate the delay time for each step.

A scenario is a step-by-step sequential description of the specific tasks or steps that the threat will implement. Develop a scenario by piecing together:

- *What* the inmate does
- *How* the inmate does it
- *How long* each task takes
- *How likely* it is that the inmate will be detected at each step

At this point PSDs and timelines will be expanded into complete scenarios. These surviving scenarios will be considered the "worst case" scenarios for the facility-- the ones in which the threat has the highest chances for success. As the scenario is described it may be necessary to collect further data and act out each step.

Caution. Testing scenarios can be very dangerous. Establish clear safety guidelines. Testing scenarios may also, under some circumstances, threaten facility security. Establish clear security guidelines before proceeding.

As performance tests are conducted for each scenario, be sure to assign JVA team members to serve as observers. Document actions and findings and also be sure to take photographs to demonstrate what was being attempted and how it turned out.

When performance tests are conducted:

- Be sure that testing does not distract an employee from his/her job
- Remember that employees will be on a heightened alert and on their best behavior
- Try to be a "fly on the wall" whenever possible
- Always be aware of safety and security issues
- Remember that inmates will almost always be watching and making their own notes

Figure 3.15 displays a format that might prove helpful as PSDs are converted into scenarios. This is useful to set up findings for entry into the EASI program for analysis.

Figure 3.15: Format for Developing Scenario Elements

Step	Path Element	Task	P_D	Delay (sec.)	Delay After Detection	Equipment
1	Door	Penetrate	.5	50	25	Hacksaw
2	Restricted Area	Cross	0	6	0	None
3	Perimeter	Climb	.9	30	30	Climbing aids/blankets

Appendix E provides several sample PSDs, scenarios and the resulting EASI findings.

B. Step 2B: Assessing Risk with the EASI Model

At last, after all the hard work, there is a tool that will do much of the remaining work. The EASI model (Estimate of Adversarial Sequence Interruption) was created by Sandia National Labs for other applications (military, nuclear weapons, atomic energy plans) and was adapted for correctional settings in the late 1990's.

EASI is provided in an Excel file that is comprised of several worksheets. Appendix I presents the formulas that are embedded in the Excel file for reference. Appendix K presents a step-by-step guide for using EASI.

The following narrative uses the threat of "escape" for illustration purposes. Of course, this process may be used successfully with many other threats.

The EASI process starts with the information that was developed in the preceding steps, specifically the scenarios with the corresponding delay and detection values. The EASI program requires additional input in the form of:

- Response force time calculations
- Pobability of successful alarm communication
- Standard deviations for times (usually entered as 20% unless data prove otherwise)
- Location of detection relative to the delay time frames (beginning, middle, end)

When all of this information is entered into EASI the reward will be a calculation of the "probability of interruption" (P_I). In other words, a statistical estimate of the odds that the facility will be able to win the race with the threat.

Figure 3.16 provides an example of an EASI timeline chart in which the inmate is interrupted before the escape time line is complete.

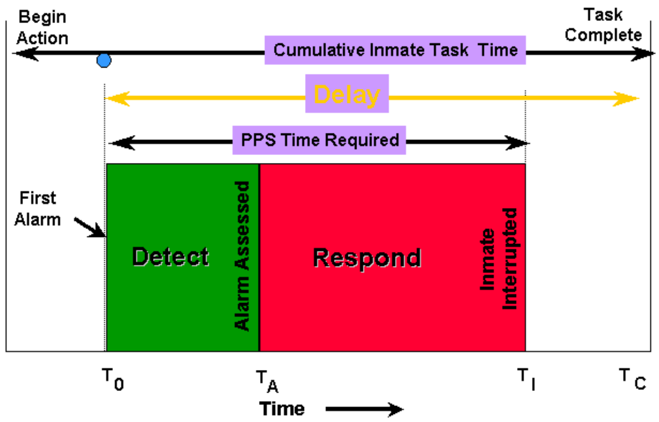
In the timeline, the inmate's actions are depicted on the top line. The actions begin before the first alarm is sounded (T_O). More time passes before the alarm is assessed (T_A) and the response is initiated. In this example, the cumulative time for detection, assessment and response is *less* than the inmate's total task time, and the inmate is interrupted (T_I). Note that the "begin action" time is not calculated. It might have taken four days for the inmate to open a hole in a wall (delay) but the timeline does not get into gear until the first alarm is encountered.

<u>Response force time</u> (RFT) is comprised of three elements:

- Alarm assessment time
- Response communication time
- Response deployment time

RFT can vary substantially depending on the scenario that is being evaluated.

Figure 3.16: Sample EASI Timeline Chart



Probability of interruption P_I) is the cumulative probability that the inmate's actions will be interrupted before the escape succeeds. Put in terms of the inmate's chances for success, the probability of inmate success would be calculated by subtracting P_I from 1. If P_I was determined to be 0.30, it would mean that 30 times out of 100 (30% of the time) the inmate would be interrupted before successfully completing the escape attempt. Expressed as the inmate's chances for success, it would be 0.70 (70 out of 100 times) the inmate would complete the escape. This is also called a measure of the risk.

Consider the following sample scenario:

1. *At 1700 hr, an inmate gets to his starting point outside the housing unit undetected.*
2. *He runs across the outer area to the perimeter fence.*
3. *Once at the perimeter fence he cuts the razor wire with cutters, cuts the inner fence with cutters, runs across the isolation zone that has a microwave sensor, cuts razor wire on the outer fence, and then cuts through the outer fence.*

A timeline is created for this scenario, in preparation for entry into the EASI worksheet, as shown in Figure 3.17.

Figure 3.17: Timeline for Scenario #1

Task Description	PD	Location	Delay time	Cum. time
Get outside housing unit	0			
Run across outer area	L	M	30	30
Cut razor ribbon	L	M	20	50
Cut inner fence	H	M	20	70
Run to outer fence	H	M	0	70
Cut outer razor ribbon	L	M	20	90
Cut outer fence	L	M	20	110

Note that the probability of detection (P_D) shown described as L (low), H (high) or O (none) in Figure 3.17. The EASI program may accept this form of data when more accurate findings are not available. The following EASI worksheet shows how the EASI program calculates the probability of interruption.

Figure 3.18: Sample EASI Worksheet

Estimate of Adversary Sequence Interruption	Probability of Alarm Communication	Response Force Time (in Seconds) Mean	Standard Deviation
	0.9	60	5

Task	Description	P (Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Run across outer area	0.1	M	30	5
2	Cut Inner Razor Ribbon	0.1	M	20	3
3	Cut Inner Fence	0.8	M	20	4
4	Run to outer Fence	0.9	M	0	0
5	Cut Outer Razor Ribbon	0.1	M	20	3
6	Cut Outer Fence	0.1	M	20	4

Probability of Interruption:	0.214819151

$\boxed{\text{Likelihood of escape is 0.79}}$

In Figure 3.18 the "description" column describes each step in the scenario. "Location" refers to the point in the delay time frame in which detection occurs (in the example the "M" stands for middle of delay period.)

The "mean" is the average number of seconds of delay that is associated with each step, and the standard deviation expresses the number of seconds (plus or minus) that the actual delay will vary from the mean.

For example, the first task, "run across outer perimeter" could be expected to take 25 to 35 seconds.

Another EASI worksheet is provided in Figure 3.19, depicting substantially different conclusions.

Figure 3.19: Sample EASI Worksheet

Estimate of Adversary Sequence Interruption

Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
0.9		75	15

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Penetrates Exterior Cell Wall	0.5	B	60	12
2	Drop to Restricted Area	0.2	B	10	2
3	Move to Containment Fence	0.2	M	20	4
4	Climb Containment Fence	0.2	M	10	2
5	Move to Inner Perimeter	0.2	M	10	2
6	Cut Shaker Wire	0.3	M	150	30
7	Cut Inner Perimeter Fence	0.1	M	300	60
8	Move through MW Zone	0.8	M	150	30
9	Cut Outer Perimeter Fence	0.4	E	205	41

Probability of Interruption:	0.953746421

Likelihood of escape is 0.05

In this example, the inmate will be interrupted before his escape 95% of the time. The inmate is interrupted early in his escape path in the second scenario, as shown in the EASI timeline in Figure 3.20.

Figure 3.20: EASI Timeline for Second Scenario, Early Interruption

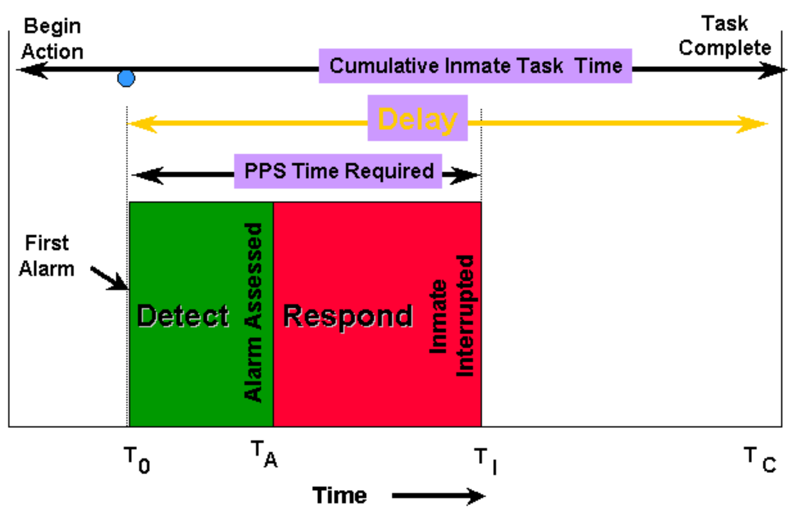
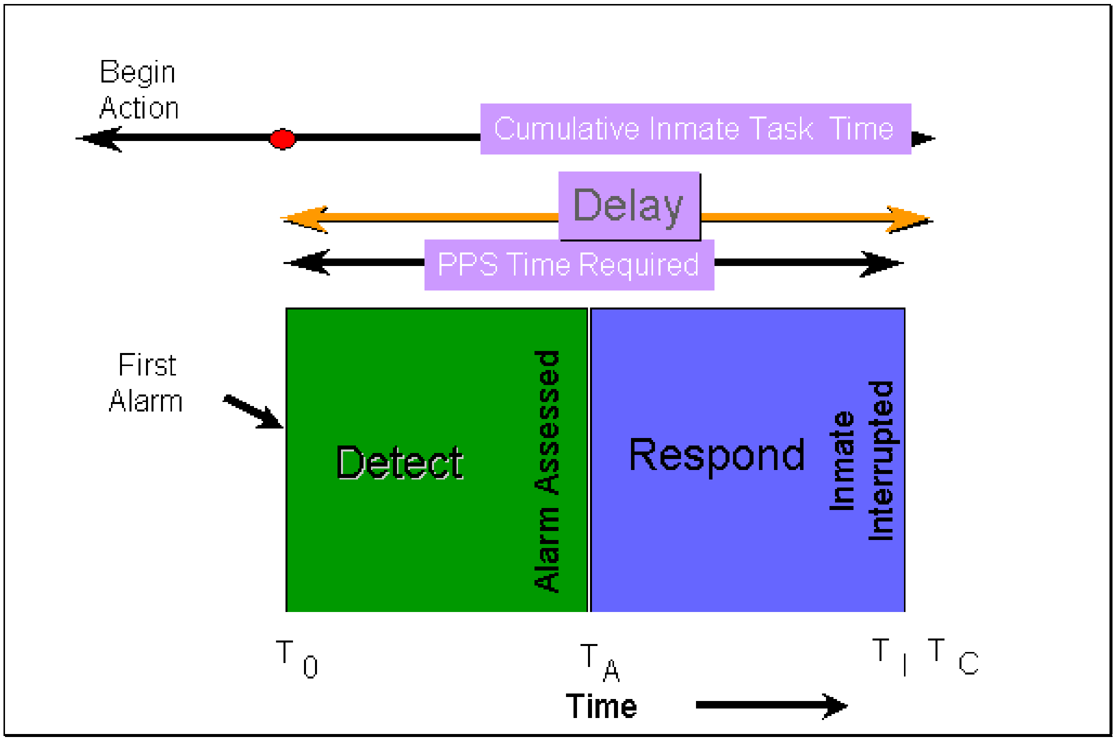


Figure 3.21 shows a timeline in which the inmate is interrupted very late in his timeline.

Figure 3.21: EASI Timeline, Late Interruption



After the EASI program has been used to evaluate each "worst case" scenario, assemble the findings for comparison and further analysis.

Consider each one of the scenarios that have been evaluated. Compare the probability of interruption (P_I) for each and then look at them as a whole. Taken together, the results for these worst-case scenarios are an indicator of the overall effectiveness of the physical protection system.

The scenarios with the lowest probability of interruption are the most important indicators of vulnerability.

<u>Using EASI to Reduce Risk</u>

EASI is a versatile tool that will help identify ways to reduce risk, and to model the impact of changes on the bottom line risk level for each scenario.

At this point in the process, for each scenario that has an unacceptable level of risk:

- Determine the reason(s) for the high level of risk
- Evaluate potential options to reduce risk
- Consider the cost associated with solutions compared with the benefits

As with the last step in Phase One, it is time to identify “root causes” for high-risk scenarios. These might include, but are not limited to:

- Inappropriate *policies* (setting out to do the wrong thing)
- Inadequate *procedures* (not attempting to do it the right way)
- Training *deficiencies* (not arming staff with the knowledge, skills and abilities they need)
- *Staffing* issues (insufficient staff, wrong type of staff assigned, inadequate deployment, etc.)
- *Equipment* shortcomings (the wrong equipment for the application, poor installation, failure to maintain the equipment, etc.)
- *Physical plant* problems (poor design, improper construction, inadequate maintenance, etc.)

When looking for root causes, expand the perspective beyond just the high-risk scenarios and:

- Consider the entire inmate range of inmates and their risk levels
- Examine scenarios and situations that are tied into or which parallel the high-risk scenarios
- Identify critical components of the PPS and the extent to which there is protection-in-depth

Using EASI to Identify *and* Test Potential Solutions

EASI not only delivers the bad news about vulnerability, it also offers a powerful tool to explore effective solutions.

The following charts use a Colorado prison scenario (see Appendix E) to demonstrate various ways in which the EASI tool may be used to identify strategies to reduce risk and to measure the impact of potential changes. Figure 3.22 presents the EASI table and the probability of interruption (P_I), which is very low. Without any changes, the inmate will succeed four out of five times.

a. Removing Tool from Scenario

The underlined words in the table identify a common <u>tool</u> that is critical to the success of the scenario -- lineman’s pliers. One of the first potential solutions to consider would be to decrease the ability of inmates to gain access to this tool by improving tool control procedures, changing the classification of the tool, increasing the security measures that control the tool, or other methods. Depriving inmates of this critical tool could result in the abandonment of the plan by the inmates. If not, it would at least make it more difficult to cut through the fences.

Figure 3.23 shows the impact of increasing the time it takes to cut the fences by a factor of two, which might happen if the lineman’s pliers were not available. The result is a reduction from 80% to 60% success for the inmate.

Figure 3.22: Sample EASI Scenario and Table

				Delays (in Seconds):	
Task	Description	P(Detection)	Location	Mean:	Standard Deviation
1	Arrive at Maintenance, retrieve tools including lineman's pliers, attack/secure staff member	0.2		120	30
2	Exit door -SV-32	0.1		5	2
	Run across dock to parked trailer	0.2		11	5
4	Hide between wheels on trailer	0.03		120	30
5	Run to internal fence and cut utilizing lineman's pliers	0.07		36	15
6	Crawl through electronic detection zone (microwave)	0.2		38	20
7	Cut fence with lineman's pliers ensuring perimeter vehicle does not detect.	0.27		73	30
8	Cross restricted area	0.2		2	1
9	Cut razor wire utilizing lineman's pliers	0.2		20	5
10	Cut fence with lineman's pliers	0.2		36	10
		Probability of Interruption: 0.19123999			
		Response Force Time (RFT): 341 seconds			

Figure 3.23: Eliminating Access to Tool, Increasing Time to Cut Fences

				Delays (in Seconds):	
Task	Description	P(Detection)	Location	Mean:	Standard Deviation
1	Arrive at Maintenance, retrieve tools, attack/secure staff member	0.2		120	30
2	Exit door -SUV-32	0.1		5	2
3	Run across dock to parked trailer	0.2		11	5
4	Hide between wheels on trailer	0.03		120	30
5	Run to internal fence and cut	0.07		72	15
6	Crawl through electronic detection zone (microwave)	0.2		38	20
7	Cut fence ensuring perimeter vehicle does not detect.	0.27		146	30
8	Cross restricted area	0.2		2	1
9	Cut razor wire	0.2		20	5
10	Cut fence	0.2		72	10
		Probability of Interruption: 0.399786467			
		Response Force Time (RFT): 341 seconds			

b. Eliminating the Trailer

Just as we removed the lineman's pliers in the preceding section (a), now we examine the impact of removing the trailer, which is used by the inmates to hide them from detection during the escape. EASI can determine the impact of removing the trailer from the yard.

For example, if removing the trailer would increase the probability of detection for steps 3 and 4 to 0.5, the EASI program will recalculate the Probability of Interruption. In this example, P_I is hardly affected, increased by only 1 percent (from 19% to 20%.) While moving the trailer might be a good idea, EASI shows that it is not the magic bullet that will foil this escape scenario.

c. Increasing the Probability of Detection

What if probability of detection is increased for other steps? Use EASI to help determine if there is a critical step at which detection would change the odds substantially. If your experiment with different probability of detection values; you will find that:

- Increasing P_D in Step 1 from 0.2 to 0.5 would increase P_I to .594
- Increasing P_D in Step 2 from 0.1 to 0.5 would increase P_I to .626
- Increasing P_D in any of the subsequent steps 0.5 would not increase P_I by even 1%!

Why would changes in detection early in the scenario yield such strong results, while comparable changes later in the sequence would have virtually no impact? Because, when it comes to detection, the major impact will be made at the earliest steps in the scenario. In this example, better detection later in the process is simply "too little, too late."

d. Improving Response Time

What about improving response time? Once again, use EASI to determine the answer. The response time for Figures 3.22 and 3.23 is 341 seconds, with a standard deviation of 70 seconds. If the response time is *reduced*, the impact on the probability of interruption would be:

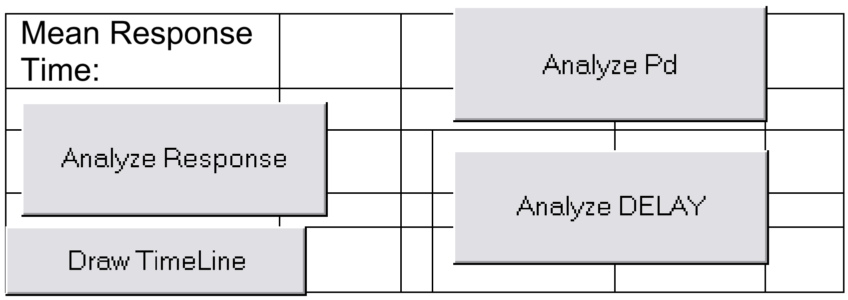
- Reduce response time to 300 seconds and P_I is 0.269
- Reduce response time to 240 seconds and P_I is 0.368
- Reduce response time to 200 seconds and P_I is 0.423
- Reduce response time to 100 seconds and P_I is 0.567

Clearly, reducing response time may have a significant impact on the probability of interruption, but it may not, by itself, be the solution that makes the odds acceptable.

E. Using the "Analyze" Buttons

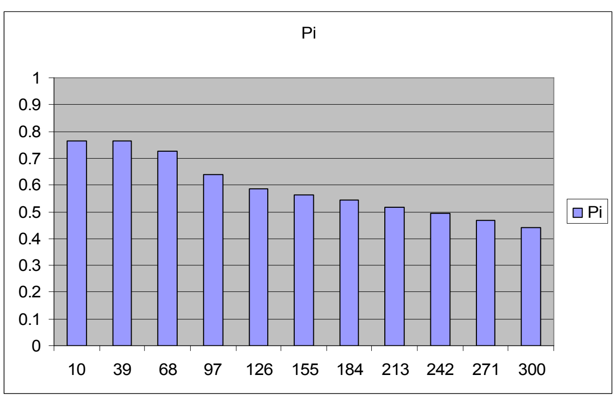
Instead of using a "trial and error" approach to determine the impact of changes in detection probabilities, delay, or response time, use the buttons on the top of the EASI worksheet. These are shown in Figure 3.24 below.

Figure 3.24: Analysis Buttons on EASI Worksheet



For example, clicking on the value for "mean response time" to the left of the buttons on the worksheet, and then clicking on the button "analyze response" will produce a worksheet entitled "response" which has a table and graph. Figure 3.25 shows the table graph that illustrate the impact on P_I for various new values of response time, using the EASI values shown in Figure 3.23. The table at the bottom of the figure presents the actual values for response time and corresponding probability of interruption.

Figure 3.25: Analysis of Response Time

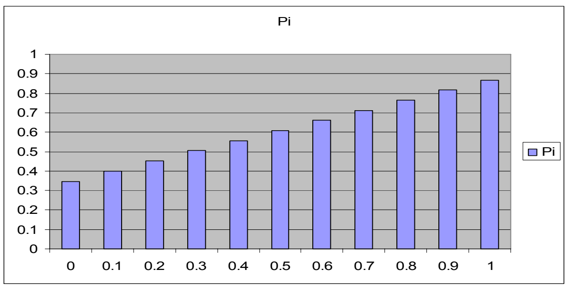


Response Time	Pi
10	0.765503972
39	0.764978365
68	0.726916876
97	0.636935273
126	0.586029427
155	0.562667188
184	0.542303314
213	0.518292249
242	0.492963593
271	0.468224653
300	0.442684083

Figure 3.25 shows the range of impact that changes in response time have on the probability of interruption. If response time is reduced to 10 seconds, P_I is 76% but that is the extent of reduction that is possible using response time.

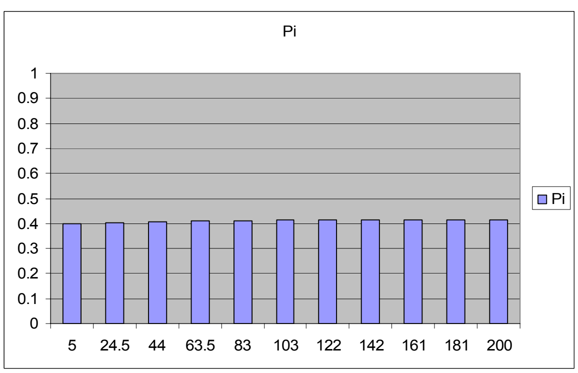
Similarly, selecting any of the values for P_D and then clicking on the "analyze P_D " button and produces a worksheet entitled "PDs" with a table and chart showing the impact of changes in P_D on the P_I . Figure 3.26 shows the graph that is created when P_D for the second step in the scenario is analyzed. It suggests that interruption may be nearly tripled if detection is improved at this early step in the process.

Figure 3.26: Analyzing Probability of Detection



The same process works for any cell containing a delay value and the "Analyze DELAY" button. Figure 3.27 shows the possible changes that would result from changing the delay values for the same step from the current 5 seconds. The graph shows that this variable is not one that will have a major impact on the overall outcomes.

Figure 3.27: Analyzing Probability of Detection



Using EASI in this manner leads to the critical element(s) that could reduce risk by changing detection, delay or response. Even better, exploring two or more changes using EASI will show a cumulative effect on risk. For example, increasing detection probabilities for Steps 1 and 2 to 0.5, along with reducing response time to 200 seconds, would produce a probability of interruption of .804, reversing the odds in favor of the facility.

The preceding examples are only a hint of the power that EASI offers as an analytical tool. By experimenting with changes in detection, delay and response, the impact on risk is instantly recalculated.

After the EASI program has yielded findings, the same process used at the end of Phase 1 is used to assemble and classify findings. Figure 3.28 presents an example of findings that might be derived from the scenario that was the subject of the preceding pages.

Figure 3.28: Sample of Findings from EASI Analysis

DEFICIENCIES	CLASSIFICATION	ROOT CAUSE
Tools are not controlled sufficiently, allowing inmates unauthorized access.	Operations	* Policies/Procedures * First Line Supervision
Exit Door SV-32 is easily compromised.	Facility	* Design/Construction
Exit Door SV-32 is not alarmed.	Technology	* Inadequate Detection Systems
There officer post located near the rear vehicle sallyport is not staffed on the third shift.	Operations	* Staffing and Deployment

The findings from Phase Two will be carried forward into the next phase of the process.

CHAPTER 4: Phase Three – Create Solutions

In this phase, all of the findings are brought together from Phase One and Phase Two. Root causes have been identified for each finding. The next step is to sort all of the findings according to their root causes.

The process through which findings are collected, classified, sorted and assigned root causes was described at the end of Phase One. Figure 4.1 describes the process.

Figure 4.1: Steps in Processing Findings

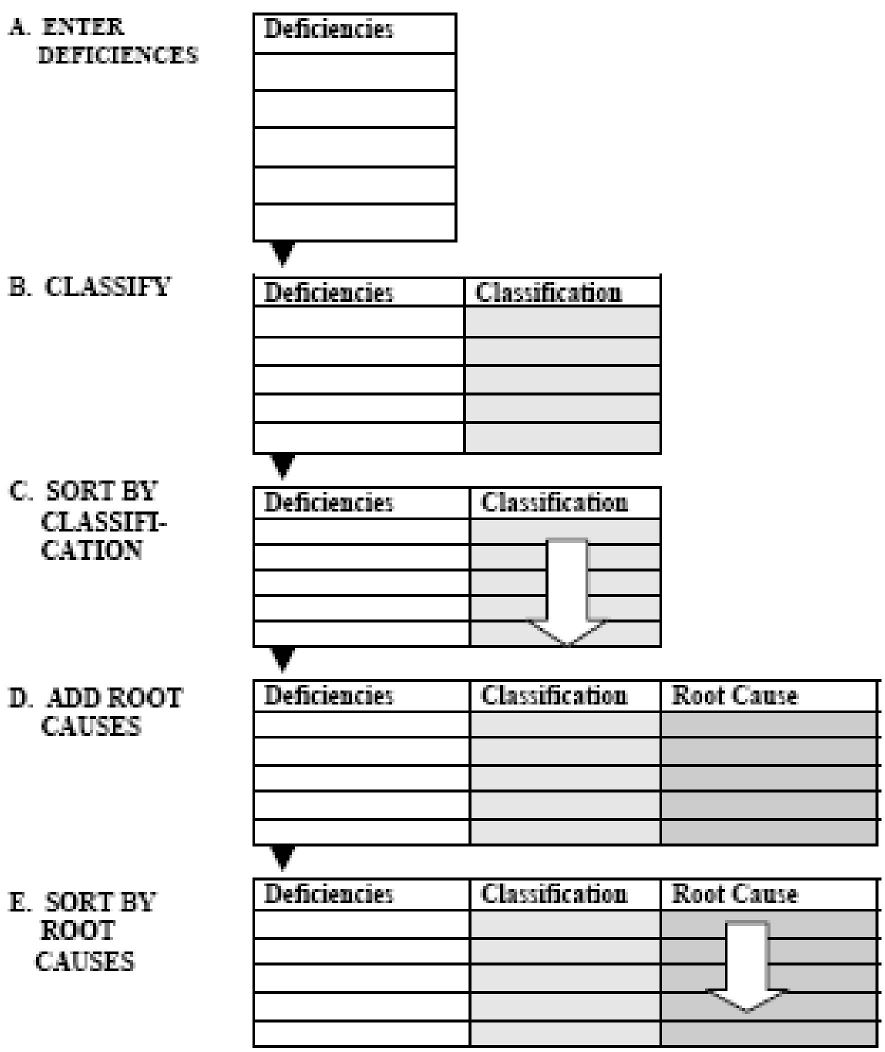


Figure 4.2 presents a sample of findings, classifications, and root causes organized according to the process.

Figure 4.2: Sample of Findings, Classification and Root Causes

DEFICIENCIES	CLASSIFICATION	ROOT CAUSE
Height of booking desk area not adequate to prevent inmate access	Facility	Design
Storage room not monitored with camera	Technology	Funding
Lock on exterior door doesn't latch	Facility	Maintenance
Drain grate in floor of holding cells have sharp or missing pieces	Facility	
Dangerous utensils (scissors) in direct line of sight of inmates	Operations	Policies/Procedures/Practice
No security officer in kitchen	Operations	Staffing
Leaving gate open allows piggybacking, contraband, escape, etc	Operations	Supervision
Kitchen utensils left unattended	Operations	
Door to holding areas equipped with electric lock, but is currently Propped open.	Operations	
Kitchen utensils left unattended	Operations	Training
Door to holding areas equipped with electric lock, but is currently propped open.	Operations	
Interlocked doors constantly being "over-ridden"	Operations	Practice

The process finally assembles the findings according to the root causes, making it easier to develop efficient and effective solutions. In this manner, dozens (if not hundreds) of individual findings eventually wind up in a manageable number of groupings. Sometimes the root cause groups will have a *variety* of classifications, although the sample in Figure 4.2 is more typical.

Note that a finding might appear in more than one root list. For example, "kitchen utensils left unattended" is entered as a supervision issue as well as a training issue. Training needs to be improved to ensure that employees know how to control utensils, but without effective supervision, the training often fades and practices fall below expected levels.

At this point, solutions will come into focus. More accurately, a series of "solution sets" will emerge describing several actions that will combine to address deficiencies.

Policies and Procedures

The JVA will likely identify instances in which current facility policies and procedures are inadequate. In some instances the procedures will be incorrect; in others, procedures might not go far enough. The need for additional policies and procedures will also be identified through the JVA. In this phase of the process, all policies and procedures should be co

Practices

The JVA will also identify instances in which policies and procedures are sound and set forth good, effective practice, but are not being followed. While a possible solution may very well involve training and supervision, it also may require a change in culture, moving toward a higher concern for security. Identifying consistent practices that defeat security systems is an important part of this process.

Training

The JVA benefits training in several ways. First, everyone who was directly involved with the JVA will have received invaluable training and insights. It is likely that their perspectives will be changed for the better. Second, facility staff members who observed JVA activities and learned about the findings will also benefit and they will be more receptive to subsequent training activities. Third, the JVA findings should be incorporated into ongoing facility training activities. Many of the deficiencies that will be identified by a JVA may be addressed by enhanced staff training.

Supervision

Many of the deficiencies that may be addressed through training will also have a supervision implication. Employee supervision is an extension of training, and should provide employees with guidance to improve compliance with policies and procedures. The American Correctional Association (ACA) has recently developed important new tools through the creation of "performance-based" standards and practices. The ACA performance-based template has several elements associated with each "expected practice." These include:

- *Protocols,* such as policies and procedures, training curricula, that describe in writing what is to be done
- *Process indicators* that identify methods to determine, on an ongoing basis, if practices are being properly implemented (an excellent supervisory tool)
- *Outcome measures* that guide the collection and analysis of data and information to determine if practices are producing the desired results

The ACA process indicators are an excellent resource to help improve continuing efforts to supervise correctional staff.

Data and Information

The JVA will have benefited from the collection and analysis of various types of data and information. After the initial JVA, data collection activities should at least continue, if not expand. Also, there were likely many instances in which data and information were not available, and the JVA was diminished as a result. These should be addressed as part of the post-JVA activities.

The ACA outcome measures should also be considered as a new tool to help determine the extent to which desired results are being realized.

Facility

Too often, we forget that the physical plant can be altered, often more easily than its operations. Many jails have used selective renovation—something as simple as putting a window in a wall—to dramatically improve staff performance.

Sometimes it may be as simple as changing the way the current facility is used; closing a housing unit, reassigning an activity to a different space, and similar use changes can also make a big difference. One jail was having trouble providing consistent supervision for attorney-client contact visits. This activity was moved to the existing non-contact visiting area, which had direct observation from a fixed control center, for contact visitation. The attorney and client use the same side of the visiting area, rather than having the glass between them.

Many simple and inexpensive renovations can significantly improve staff efficiency. These changes can address operational issues:

- Observation—adding observation windows, improving sightlines, creating an observation room adjacent to an existing post.

- Separation—increasing the ability to separate inmates in housing and activity areas.

- Movement—providing more secure compartments in the jail, relieving concerns about allowing inmates to move without escort.

Relocating activities, such as fixed control posts, may seem expensive, but these one-time renovations may be more cost-effective than adding staff for the life of the facility. Sometimes it is just a matter of changing fixtures or furnishings. Replacing a solid steel door with one that has a vision panel can make a big difference in observation and sightlines. Improving lighting is another way to improve observation and surveillance. Think of your facility as a work in progress. Be aggressive when analyzing problems and identifying opportunities to adapt the facility to serve your operations better.

As with previous phases, this process works best when stakeholders have many opportunities to participate. Take the time to ensure maximum involvement.

CHAPTER 5: Phase Four - Implementing Solutions

In many ways, completion of the JVA is only the beginning. A comprehensive action plan should describe specific steps to be taken, time frames, and responsibilities.

Liability

Liability should be a continuing concern. Failing to effectively address identified problems will increase liability. Every official, at all levels, should do everything within his/her power to act effectively to make improvements. Officials should address *every* issue and vulnerability that was identified through the JVA. These will include the elements of the scenarios, and also the various findings and observations that were not attached to specific scenarios.

Testing

The JVA will spotlight the need to improve ongoing efforts to test elements of the physical protection system. The lessons from the JVA should be translated into improved testing practices. Some agencies have incorporated intermittent testing into their procedures and post orders.

Reporting

It is important to gather your findings and recommendations into a comprehensive report. A sample report from a Colorado prison is presented in Appendix L. Much of the text from this handbook might also prove useful, and readers are encouraged to draw from it, with attribution.

Utilizing JVA for Budgeting

It is likely that some of your solutions will involve funding. The budget process is an ideal forum to utilize the data collected and insights gained. Some of the more objective data, such as EASI, may be used to justify allocation requests. For example:

> *I am requesting the addition of 6 correctional officer positions. Through the JVA process, we discovered that the chance of an adverse event (name 1) to be successful is 1 in 3 attempts, potentially risking public safety. However, with the addition of the requested staff, we can reduce the response time to the event, and ultimately reduce the odds of success to 1 in 10.*

Training

The employees who are responsible for delivering and developing staff training are an essential part of a JVA team. At the conclusion, when all the information is compiled and analyzed, the training staff examine at it from a training perspective. Starting with root causes, specific training needs areas may be identified. Beyond that, training curricula may be developed.

Developing a "Security Culture"

The goal of the JVA process is to develop and empower employees at all levels to improve safety and security, and to be involved with continuous security improvement. In jails, where we often achieve security through operational practices and often rely less on technology and the facility, it is especially important that a "culture of security" permeates the entire facility. The JVA process may be used to generate a road map that leads the agency toward better practices.

= =

Appendices

Appendix A: Threat Capability Checklists

Appendix B: Checklists for Characterizing the Institution

Appendix C: Physical Protection System Checklists

Appendix D: Protocols and Practices

Appendix E: Sample PSD’s and EASI Results

Appendix F: Data Collection Forms (Entry Control, Delay)

Appendix G: Performance Data Tables

Appendix H: Path Sequence Diagram (PSD) Checklist

Appendix I: Acronyms and Selected EASI Formulas

Appendix J: Excerpts from *Core Jail Standards*

Appendix K: A Step-by-Step Guide to Using the EASI Program

Appendix L: Sample Report from Prison VA

Appendix M: A Primer on Physical Protection Systems (PPS)

Appendix N: Powerpoints from a Four-Day JVA Training Program

Appendix A: *Sample* Threat Definition Checklist

√	**Incidents?**	**Comments (reference to Checklists in Appendix D)**
	Escape	
	1. Identify any past incidents and describe the details of the scenario presented by the inmate(s).	Ref. A4. Intelligence
	2. Details should include a description of inmate tactics, weapons, escape path elements, tools used, transportation, the time of day, and weather. Was the inmate(s) acting in collusion with anyone from the outside and/or staff?	Ref. A4. Intelligence
	3. Escape attempts can be accomplished by using either one or all of the following methods, deceit, force, and stealth. The analyst should identify which method(s) was used in the attempt.	Ref. A4. Intelligence
	4. Determine historical data, i.e. past/present/future, using past records and intelligence information.	Ref. A4. Intelligence
	Contraband	
	1. Determine the type of contraband that is being brought into the facility, i.e. weapons, drugs, money, electronic devices.	Ref. A4. Intelligence
	2. Identify the means in which the contraband is being introduced into the facility, i.e. visitor areas, daily deliveries, and staff.	Ref. A4. Intelligence
	3. Determine the means in which the contraband is being packaged.	Ref. A4. Intelligence
	4. Determine the ownership of the contraband and if it is associated with a specific group or activity.	Ref. A4. Intelligence
	5. Determine historical data, i.e. past/present/future, using past records and intelligence information.	Ref. A4. Intelligence

	Suicide	
	1. Inmates should be identified as potential suicide risks.	
	2. Processes should be in place to establish suicide threat watch.	
	3. Determine historical data, i.e. past/present/future, using past records and intelligence information on suicides in the facility.	
	4. Identify specific locations (physical room layout) where suicides can and has occurred.	
	5. The type of weapons used in committing the act.	
	6. Details should include a description of inmate tactics, weapons.	
	7. Was the inmate acting in collusion with anyone from the outside and/or staff?	
	Inmate Violence	
	1. The types of inmates that are housed in the facility and locations, i.e. maximum/medium/minimum.	
	2. The type of violence, i.e. individual, gang (number of subjects), and against the staff.	
	3. The time of the occurrence and whether it was day or night.	
	4. Determine the frequency and severity that violence occurs.	
	5. Determine historical data, i.e. past/present/future, using past records and intelligence information.	
	6. Identify specific locations (physical room layout) where violence can and has occurred.	
	7. The type of weapons used in committing the acts.	

APPENDIX B: CHECKLISTS for Step 1B- Identifying Problems and Concerns

Physical Characteristics and Features

Inventory B1: Location

This inventory focuses on the location of the facility within the broader context of the neighboring activities and features. It looks at what is located near and nearby the site.	Check Y when completed	**Comments**
Part 1: On an <u>area map</u>, identify: a. the location of the facility		
b. **r**outes to and from the facility		
c. nearby transportation routes/complexes (roads/highways, waterways, railroads, airports).		
Part 2: Vulnerability Analysis Using the map created in Part 1, identify and describe potential vulnerability in terms of: a. <u>Proximity/Adjacency</u> What might pose a threat because it is *nearby* the facility site? What might pose a threat because it is *next to* the facility site*?*		[Sample findings] Private airport located .7 miles northeast of the site could provide base of operations for helicopter. State forest that abuts the perimeter on the west side of the site provides cover for escapee and/or persons assisting escape from the outside
b. <u>Visibility/Observation</u> (1) Identify blind spots, poor lines of sight, obstructions and other features that might pose a threat. (2) Identify environmental conditions (e.g. rain, fog, snow, etc.) that affect visibility and observation.		[sample findings] Topography on of the area to the southwest of the site creates blind spots that prevent a vehicle from being observed before it reaches the site. Poor visibility of county road to the north side during rain, fog and snow.

Inventory B2: Site

This inventory focuses on the features of the *site* on which the facility is located.	Check Y when completed	**Comments**
Part 1: On a **site plan**, identify the following: a. Property boundaries		
b. Roads and pedestrian circulation		
c. Land uses of adjacent parcels (e.g. residential, commercial, industrial, etc.)		
d. Parking lots and assigned users.		
e. Footprint of all buildings on the site.		
f. Major topographical features, including man-made features such as draining ditches.		
g. Location of all subsurface utilities and other systems (e.g. power, water, sanitary waste, storm sewers, utility tunnels, etc.)		
h. Emergency access and holding areas (e.g. access for fire trucks, yards used to evacuate inmates from the facility, etc.)		
i. Location and type of external security fences and walls.		
Part 2: Vulnerability Analysis Using the site plan created in Part 1, identify and describe potential vulnerability in terms of: a. Proximity/Adjacency What features on the site pose a threat because they are *near* each other? What feature on the site pose a threat because they are *next to* each other?		[Sample findings] Storm drain entrance near the west fence. Facility wall next to the east fence line creates escape risk.

Inventory B2 (continued)	Check Y when completed	**Comments**
b. <u>Visibility/Observation</u> (1) Identify blind spots, poor lines of sight, obstructions and other features on the site that might pose a threat. (2) Identify environmental conditions (e.g. rain, fog, snow, etc.) that affect visibility and observation on the site.		[sample findings] Topography of the north west area inside the perimeter fences creates opportunity for contraband to be hidden. Lines of site on north and east perimeter are inadequate during rain, fog and snow.
c. <u>Continuity</u> Identify instances in which continuity of features or systems is interrupted on the site.		[sample finding] Perimeter patrol road is not complete on south side.
d. <u>Condition</u> Identify features on the site whose condition poses a potential threat.		[sample finding] Security grates on storm sewer entrance (SW side) are in poor condition.

Inventory B3: Facility Design, Layout and Construction

This inventory focuses on the characteristics of the facility itself-- the way it is designed, its overall layout, and the types of construction.	Check Y when completed	**Comments**
Part 1. **A. Facility Design and Layout.** On one or more facility floorplan(s), identify the following: (1). *Access and egress* points and the types of users that are authorized (e.g. public, staff, deliveries, inmate transport, etc.)-- (a) Pedestrian		
(b) Vehicle		
(2) Security perimeter.		
(3) Pedestrian and vehicle sallyports.		
(4) Other doors or gates that penetrate the security perimeter (not included in c. above)		
(5) Utility entrance panels, utility and mechanical rooms and equipment. Include emergency generator(s).		
(6) Location of emergency/security equipment (e.g. armory, storage of air packs, etc.)		
(7) Rooms containing communications equipment.		
(8) Rooms containing data and information systems equipment.		
(9) Rooms that contain medical supplies and drugs.		
(10) Rooms that contain tools and equipment and key with description of types of contents.		
(11) Rooms that contain other items that might be used by inmates to threaten safety/security (e.g. free weights, etc.)		

Inventory B3 (continued)	Check Y when completed	**Comments**
B. <u>Facility Construction</u>. On one or more facility <u>floorplan(s)</u>, identify the following: (1) Each variation of wall construction used in the facility. Use a legend to show where each type of construction is found.		Note: If there is a consistent pattern for the use of each element throughout the facility, floorplans need not be marked in detail (e.g. if all windows within the secure perimeter of a certain type, etc.)
(2) Each variation of floor construction, using a legend to show where each type is found.		
(3) Each variation of ceiling construction, using a legend to show where each type is found.		
(4) Each variation of roof construction, using a legend to show where each type is found.		
(5) Each variation of window construction, using a legend to show where each type is found.		
(6) Each variation of door construction, using a legend to show where each type is found.		
Part 2: Vulnerability Analysis Using the <u>floorplan(s)</u> created in Part 1, identify and describe potential vulnerability in terms of: a. <u>Proximity/Adjacency</u> What facility characteristics pose a threat because they are *near* each other? What facility characteristics pose a threat because they are *next to* each other?		[Sample findings] Correctional industry shops located near vehicle sallyport. Proximity of maintenance shop to housing units.
b. <u>Visibility/Observation</u> (1) Identify blind spots, poor lines of sight, obstructions and other facility characteristics that might pose a threat. (2) Identify environmental conditions (e.g. rain, fog, snow, etc.) that affect visibility and observation in the facility.		[sample findings] Secondary corridor in program area creates several blind spots. Interior courtyards not able to be observed fully in heavy snow.

Inventory B3 (continued)	Check Y when completed	**Comments**
c. Continuity Identify instances in which continuity of facility characteristics are interrupted in the facility.		[sample finding] Reinforced concrete construction is not continued in exterior walls of housing unit B.
d. Condition Identify facility characteristics whose condition pose a potential threat.		[sample finding] Security ceiling in program areas has deteriorated to the point that it can be breached.

Inventory B4: <u>Video Systems</u>

This inventory focuses on the video systems that are used in- and around- the facility.	Check Y when completed	**Comments**
Part 1: On one or more <u>**floor plan(s) and site plan(s)**</u>, record the following: a. Location and type <u>every</u> video *camera* installation in the facility and on the site. *Use <u>Form B4-1a</u> to describe each type of camera installation.*		
b. Location and type <u>every</u> video *monitoring* installation in the facility and on the site. *Use <u>Form B4-1b</u> to describe each type of monitor installation.*		
Part 2: Vulnerability Analysis Using <u>floor plan(s) and site plan(s)</u> created in Part 1, identify and describe potential vulnerability in terms of: a. <u>Proximity/Adjacency</u> What video installations pose a threat because they are *near or next to* something else?		[Sample findings] Camera 12-c is near the laundray exhaust vent and often fogs up in cold weather. Camera 2-f is next to a stair that is accessible to inmates and could be compromised easily.
b. <u>Visibility/Observation</u> (1) Identify blind spots, poor lines of sight, obstructions associated with specific video installations that might pose a threat. (2) Identify environmental conditions (e.g. rain, fog, snow, etc.) that affect visibility and observation for specific video installations.		[sample findings] Camera 7-d is partially obstructed when the garbage truck is parked in the north vehicle parking area. Cameras 5a through e are not functional during periods of fog and snow.

Inventory B4 (continued)	Check Y when completed	**Comments**
c. <u>Continuity</u> Identify instances in which continuity of features or systems are interrupted in the facility and/or on the site.		[sample finding] Areas of the perimeter fence onf the east side are not covered by any cameras.
d. <u>Condition</u> Identify specific installations whose condition pose a potential threat.		[sample finding] Frequent breakdowns experienced in cameras 3-a, 14-c and 15-d.

FORM B4-1a: <u>Video CAMERA Installations</u> (supplement for Inventory B4)

CAMERA INSTALLATIONS:	Complete a column for *each <u>type</u> of* camera installation. For example, all perimeter cameras might be the same type of installation (same expectations and characteristics); all of these would be record in one column. Use additional pages as needed.			
(a) <u>Identifier.</u> Assign a unique code to each type of installation. Record the code number on floorplan(s) and/or site plan(s) described in Inventory B4, Part 1, a	[sample] V1- interior cameras at corridor doors	[sample] V2- exterior cameras mounted on building	[sample] V3- cameras in housing unit dayrooms	
(b) <u>Expectations of Camera Installation</u>. **<u>(1) Primary Function</u>** Use the following codes to identify the primary expected functions for each type of camera installation. **A=** alarm (e.g. motion-activated) **AA=** alarm assessment **S=** surveillance RECORD ALL THAT APPLY.				
(2) <u>Type of Threat.</u> Use the following codes to identify the expected types of threats to be identified by each type of camera installation. **V=** Violence **E=** Escape **C=** Contraband **D=** Destruction (prop) RECORD ALL THAT APPLY.				
(3) <u>Degree of Detail</u>. Use the following codes the identify the degree of detail that is expected for each type of camera installation. **D= Detect** that something is in the scene provided by the camera **C= Classify** what is in the scene-- e.g. human vs. small animal **R= Recognize** the identify of a person in the scene (RECORD ONLY ONE CODE)				
(4) <u>Camera Capabilities.</u> Use the following codes to identify the expected camera capabilities for each type of camera installation. **P=** Pan (move back and forth on command) **T=** Tilt (move up and down on command) **Z=** Zoom (move in an out on command) RECORD ALL THAT APPLY				

FORM B4-1b: <u>Video CAMERA Installations</u> (supplement for Inventory B4)

MONITOR INSTALLATIONS:	Complete a column for *each* monitor installation. For example, one monitor installation my be in master control, another in a housing unit sub-control, and a third might be in an administrative office. Use additional pages as needed.			
(a) <u>Identifier</u>. Assign a unique code to each installation. Record the code number on floorplan(s) and/or site plan(s) described in Inventory B4, Part 1, a	[sample] M1- master control center	[sample] M2- housing unit B sub-control	[sample] M3- Dep. Warden, Security, office	
(b) <u>Expectations of Monitor</u>. **(1) <u>Degree of Detail</u>.** Use the following codes the identify the degree of detail that is expected for each monitor installation. **D= Detect** that something is in the scene provided by the camera **C= Classify** what is in the scene-- e.g. human vs. small animal **R= Recognize** the identify of a person in the scene (RECORD ONLY ONE CODE)				
(2) <u>Camera Capabilities.</u> Use the following codes to identify the expected camera control capabilities at each camera installation. **P**= Pan (move back and forth on command) **T**= Tilt (move up and down on command) **Z**= Zoom (move in an out on command) RECORD ALL THAT APPLY				
(c) Characteristics of Monitor Installation **(1) <u>Continuous Power?</u>** Use codes. **0**= No (none) **B**= battery backup **G**= emergency generator .				
(2) <u>Recording Capabilities</u>, Use code. **0**= None **D**= Digital **F**= Frame Capture **R**= Real-Time **TL**= Time Lapse				
j. <u>Activation of Recording</u>. Use code. **M**= Manual **A**= Automatically **S**= Sensor-related				

Inventory B5: <u>Alarm and Sensor Systems</u>

This inventory focuses on the alarm and sensor systems that are used in- and around- the facility.	Check Y when completed	**Comments**
Part 1: On one or more **<u>floor plan(s) and site plan(s)</u>**, record the following: a. Location and type <u>every</u> distinct sensor installation in the facility and on the site. *Use <u>Form B5-1a</u> to describe each <u>type</u> of sensor installation.*		
b. Location and type <u>every</u> alarm communication and display installation in the facility and on the site. *Use <u>Form B5-1b</u> to describe each type of alarm installation.*		
Part 2: Vulnerability Analysis Using <u>floor plan(s) and site plan(s)</u> created in Part 1, identify and describe potential vulnerability in terms of: a. <u>Proximity/Adjacency</u> What sensor and alarm installations pose a threat because they are *near or next to* something else?		[Sample findings] Camera 12-c is near the laundray exhaust vent and often fogs up in cold weather. Vibration from closing of interior vehicle sallyport gate often triggers Sensor S2-9.
b. <u>Performance</u> (1) Identify physical conditions and operational situations that interfere with the performance of sensor and alarm installations. (2) Identify environmental conditions (e.g. rain, fog, snow, etc.) that affect the performance of sensor and/or alarm installations.		[sample findings] Sensor S3-1 registers a false alarm when power is temporarily interrupted. Sensor S7-3 does not function during heavy rain.

Inventory B5 (continued)	Check Y when completed	**Comments**
c. Continuity Identify instances in which continuity of the sensor and/or alarms are interrupted in the facility or on the site.		
d. Condition Identify sensors and alarms whose condition poses a potential threat.		

FORM B5-1a: <u>Sensor Systems Installations</u> (supplement for Inventory B5)				
SENSOR SYSTEM INSTALLATIONS:	Complete a column for *each <u>type</u> of* sensor system installation. Use additional pages as needed.			
(a) <u>Identifier</u>. Assign a unique code to each type of installation. Record the code number on floorplan(s) and/or site plan(s) described in Inventory B5, Part 1, a				
(b) <u>Characteristics of Sensor Installation</u>. **(1) <u>Type of Sensor</u>.** Use the following codes the identify the type of sensor. **I= Interior** **E= Exterior**				
(2) <u>Sensor Technology</u> Use the following codes to identify the type of technology for each type of sensor installation. **M=** Microwave **A=** Active Infra Red **P=** Passive Infra Red **B =** Buried Cable **U =** Ultrasonic **F =** Fence Disturbance **O -** Other (describe here: ________________ ________________________________)				

FORM B5-1b: **<u>Alarm Communication and Display Installations</u>** (supplement for Inventory B5)

ALARM COMMUNICATION AND DISPLY INSTALLATIONS:	Complete a column for *each* alarm communication and display installation (each location.) Use additional pages as needed.			
(a) <u>Identifier</u>. Assign a unique code to each type of installation. Record the code number on floorplan(s) and/or site plan(s) described in Inventory B5, Part 1, b				
(b) <u>Characteristics of Alarm Communication and Display Installation</u>. **(1) <u>Communication Lines</u>.** Use the following codes the identify the type of communication between the sensor(s) and alarm display. . **W = Wire** **F = Fibre Optic** **O = Other** (describe here: __________ ________________________.) ENTER ALL THAT APPLY				
(2) <u>Operator Interface</u> Use the following codes to identify the type of operator interface for each installation. **A = Audible** **M = Maps** **G = Graphics** **L = Lights** **O -** Other (describe here: _______________ _____________________________) RECORD ALL THAT APPLY				

Inventory B6: <u>Metal and Other Detectors</u>

This inventory focuses on the various detector equipment that is available in the facility.	Check Y when completed	**Comments**
Part 1: On one or more **<u>floor plan(s) and site plan(s)</u>**, record the following: a. Location and type <u>every</u> metal and other detector installation in the facility and on the site. *Create a legend to identify the <u>type</u> of detector.*		
Part 2: Vulnerability Analysis Using <u>floor plan(s) and site plan(s)</u> created in Part 1, identify and describe potential vulnerability in terms of: a. <u>Proximity/Adjacency</u> What detector installations pose a threat because they are *near or next to* something else?		
b. <u>Performance</u> (1) Identify physical conditions and operational situations that interfere with the performance of detector installations. (2) Identify environmental conditions (e.g. rain, fog, snow, etc.) that affect the performance of detector installations.		
c. <u>Condition</u> Identify detector installations whose condition poses a potential threat.		

Operational Characteristics

Inventory B7: Operations

Documentation / Information	√	Reference to Appendix D Operational Checklists
1. Manpower Surveys, Staffing Patterns, Schedules Manpower needed for special conditions: day, night, holidays, etc.		**Ref. A1. Staffing**
• Length and number of day and night shifts		
• The number of Correctional Officers available during each shift and holiday		
• Availability of special response teams		Ref. A3. Emergency Preparedness
2. Historical Reports (past/present/future)		**Ref. A4. Intelligence**
• Identify the meteorological conditions for the region and time of the year		Ref. A4. Intelligence
• Identify incidents that have occurred (i.e. escape attempts, class 1 contraband, etc.), and specifically develop a detailed model of how the event occurred		Ref. A4. Intelligence
• Determine if any intelligence has been developed that indicates any future activities and how it could be accomplished		Ref. A4. Intelligence
• Identify the number of inmates and their classification		A2. Inmate Accountability
• Extraordinary Reports (PADOC specific type report)		Ref. A4. Intelligence
• Misconduct Information		Ref. A4. Intelligence
3. Site Detection/Delay/Assessment Systems		**Ref. B. Equipment and Technical Systems**
• Existing means of physical protection		Ref. B. Equipment and Technical Systems
• Location of vital information that could cause a breach in security or other serious consequences		
• Identify and describe the type of materials that compose the roof, walls, windows (bars), floors, foundation, ventilation ducts, sewage and water supply		Ref. B3. Building Layout and Construction.
• Identify old and outdated equipment and the prospect for future upgrades		Ref. B. Equipment and Technical Systems

Documentation / Information	√	**Reference to Appendix D Operational Checklists**
<u>4. Weapons Inventory</u>		**Ref. C4. Armory**
• Location and number of weapons available to the Correctional Officers		
<u>5. Operational Procedures</u>		**Ref A. Operations**
• Building locations and characteristics, i.e. describe the purpose of the building, who is allowed access and its operational conditions		Ref. C1. Location and Site Ref. C2. Building Layout and Construction Ref C3. Entrances and Exits in the Secure Perimeter
• Location of inmate work details and the number and classification of the prisoners		Ref. A2. Inmate Accountability Ref. A7. Transportation of Inmates
• Allowing access to the facility by contractor/vendors		Ref. B6. Locking Systems Ref. B7. Control Center Ref. C3. Entrances and Exits in the Secure Perimeter
• Inmate transfers to locations inside and outside of the facility		Ref. A6. Visiting, Ref. A7. Transportation of Inmates
• Operational procedures dealing with inmate activities, i.e. privileges, visitors, and sport, etc.		Ref. A6. Visiting
• Access control to include inspection of vehicles and personnel		Ref. A5. Searches Ref. B6. Locking Systems Ref. B7. Control Center Ref. C3. Entrances and Exits in the Secure Perimeter
• Accountability of inmates		Ref. A2. Inmate Accountability
• Procedures on issuing of weapons and accountability		Ref. C4. Armory
• Correctional Officer post orders and operational instructions		A1. Staffing A9. Training

Documentation / Information	√	Reference to Appendix D Operational Checklists
<u>6. Policy Requirements</u>		**Policies and Procedures Guideline for correctional facilities**
• Policies related to facility security and control (reference Volume 6 Security Policy and Procedures)		
<u>7. Performance Test Data</u> Results of all tests conducted on physical and technical systems (e.g. backup generator tests, fence alarm tests, etc.)		
<u>8. Security Inspection Results</u> Results from inspections conducted by institutional staff or outside entities.		**Ref. A8. Security Inspections**

Appendix C: Physical Protection System (PPS) Checklists

The following checklists will help guide you through your review of facility detection, delay and response capabilities. References are provided to the

DETECTION

To prevent undesirable events, they must first be detected. Following are some areas that should be identified and understood to evaluate the detection capabilities of a PPS.

√	**Tasks**	**References (see Appendix D)**
	Detection	**Ref. B. Equipment and Technical Systems**
	Identify the type of entry control systems in place, i.e. badge, personnel identification, card readers, metal detectors, and state opportunities for piggybacking	Ref. B3. Metal and Other Detectors Ref. B6. Locking Systems Ref. B7. Control Center
	Determine the process for key control, combination locks and seals	Ref. B6. Locking Systems
	Identify how packages are allowed into the facility, i.e. x-ray, open and visually search	Ref. A5. Searches Ref. B3. Metal and Other Detectors Ref. C5. Mail Room
	Documented procedures used to allow access or departure	Ref. A6. Institution Visiting Ref. A7. Transportation of Inmates Ref. B6. Locking Systems Ref. B7. Control Center
	Identify and describe the perimeter to include boundaries, fence fabric, gates, sensors (location interior/exterior), length and width of clear zone	Ref. B5. Perimeter Fence Ref. C3. Entrances and Exits in the Secure Perimeter
	Determine the protection level for the security system's infrastructure	Ref. B4 Physical Plant Security
	Determine system reliability	Ref. B. Equipment and Technical Systems
	Identify the integration between detection and assessment	Ref. B1. Video Systems Ref. B2. Alarm and Sensor Systems Ref. B5. Perimeter Fence
	Determine the physical and environmental conditions as they relate to PPS	Ref. B. Equipment and Technical Systems Ref. C. Physical Plant
	Past/Present/Future results from known defeat methods, and records related to system performance	Ref. A4. Intelligence
	Performance testing related to assessing situations and emergency incidents	Ref. A3. Emergency Preparedness Ref. A8. Security Inspections Ref. A9. Training

√	Tasks	References (see Appendix D)
	Identify the present video systems in place and related components (switching equipment/video playback/video monitors/controller/ transmission medium/and monitor location for rapid and immediate assessment)	Ref. B. Equipment and Technical Systems
	Assessment by observation, i.e. CO's in towers, monitoring stations (protection level), and ability to signal duress	Ref. A3. Emergency Preparedness Ref. B1. Video Systems Ref. B5. Perimeter Fence
	Identify other responsibilities that could reduce assessment capabilities, i.e. respond to alarms, paperwork, and key service	Ref. B. Equipment and Technical Systems
	Identify the information available to the CO on the display board	Ref. B1. Video Systems Ref. B2. Alarm and Sensor Systems Ref. B5. Perimeter Fence
	Determine the process used in establishing a secondary monitoring station	Ref. B1. Video Systems Ref. B2. Alarm and Sensor Systems Ref. B5. Perimeter Fence

Delay

An effective physical protection system requires that any malevolent act committed must be detected so that CO response can interrupt and neutralize the situation. The types of delay employed at Correctional Institutions can vary from the correctional officer to locks, fences and razor wire.

√	Tasks	Comments
	Delay	Ref. B. Equipment and Technical Systems Ref. C. Physical Plant
	Identify the type of fences and gates surrounding the facility	Ref. B5. Perimeter Fence Ref. C2. Building Layout and Construction Ref. C3. Entrances and Exits in the Secure Perimeter
	Vehicle barriers	Ref. B5. Perimeter Fence Ref. C2. Building Layout and Construction Ref. C3. Entrances and Exits in the Secure Perimeter
	Construction of walls/ windows/doors/roofs/floors	Ref. C2. Building Layout and Construction Ref. C3. Entrances and Exits in the Secure Perimeter
	Identify areas where detection is not provided	Ref. B. Equipment and Technical

	before delay	Systems Ref. C. Physical Plant
	Determine if multiple layers of delay exist, i.e. locks, windows, walls, distance, fences, and razor wire (are they balanced)	Ref. B. Equipment and Technical Systems Ref. C. Physical Plant

Response

An effective physical protection system requires a response to prevent the acts from occurring.

√	**Tasks**	**Comments**
	Response Force	**Ref. A3. Emergency Preparedness**
	The type of communication available to CO's and backup types	Ref. A3. Emergency Preparedness
	Internal communication system for major events, i.e. sirens, duress alarms, public address systems, timely and accurate	Ref. A3. Emergency Preparedness
	Operator's ability to assess activity, i.e. ergonomics, accessibility to equipment, space availability	Ref. A3. Emergency Preparedness
	Review response timeline and establish timelines in accordance with the threats	Ref. A3. Emergency Preparedness
	Identify the type of response force plans/training (physical and tactical)/performance tested/ratio of CO's to inmates	Ref. A3. Emergency Preparedness
	Identify the number and type of primary responders for a given threat and the number and number of secondary responders should the need arise	Ref. A3. Emergency Preparedness
	Determine post and patrol locations and responsibilities in locating / verifying / isolating / containing / evacuating / resolving / de-activating situations	Ref. A3. Emergency Preparedness
	Implementing compensatory measures when FAR/NAR is excessively high	Ref. A3. Emergency Preparedness
	Response force armed vs. unarmed, training and checkout procedures. Equipment appropriate for the assigned task	Ref. A3. Emergency Preparedness
	CO's ability to monitor diversionary tactics, and identify policies in places that address these tactics	Ref. A3. Emergency Preparedness
	Interview senior CO's and identify additional areas for consideration	Ref. A3. Emergency Preparedness

APPENDIX D:

MANUAL OF JAIL SECURITY PROTOCOLS AND PRACTICES

Adapted from material developed by the American Correctional Association through a grant from the National Institute of Justice, Office of Justice Programs, U.S. Dept. of Justice, for use in the *Correctional Vulnerability Handbook* (2006).

I: INTRODUCTION

A. Introduction

This document offers a tool for professionals who operate jail facilities. It is designed to identify physical and operational strengths and weaknesses that pose a threat to institutional security--that make the facility *vulnerable*.

Initially developed by correctional practitioners and security experts for use in prisons, this document reflects the diverse experience of the authors, combined with the insights and suggestions of many who have volunteered to review and test it in the field. It has been adapted for use in jails as a part of the Jail Vulnerability Assessment Handbook.

Sandia National Laboratories (SNL) brought a wealth of technical expertise to the prison version of this document. Their longstanding efforts for the Department of Energy, assessing the security of nuclear power stations, produced many new instruments and a methodology for evaluating vulnerability. Subsequent SNL work for the Pennsylvania Department of Corrections provided the opportunity to transpose and adapt earlier work to correctional settings.

This document was also informed by the Federal Bureau of Prisons "Total Management System" (TMS). Many states have similar management systems.

This document represents an attempt to strike a balance between the need to be thorough and the limitation of staff time that is available to implement a vulnerability assessment. For example, an exhaustive inventory of video technology in a typical federal maximum security facility, using SNL protocols, would produce over three hundred pages of descriptive material. In this document we have attempted to capture the essential elements of such an inventory without creating a volume of work that makes it less feasible for a typical jail to complete the assessment.

We have also attempted to strike a balance between the operational dimensions of security and the technical elements and systems. On the operational side, it was often difficult to identify those operational practices that have a strong connection to vulnerability; it is arguable that virtually all aspects of facility operations contribute to overall security.

B. Principles of Security

Achieving and maintaining jail security is a full time endeavor. It demands the coordinated efforts and continuous vigilance of staff, and a supportive physical setting.

Achieving security, and thereby reducing vulnerability, is a unique challenge for each jail. No two facilities present the same physical and operational characteristics. Each setting poses unique physical and technical deficiencies, for which daily operations must compensate.

According to one text [1], a "healthy security program is based on a variety of carefully integrated factors and conditions" that include:

- fundamental and clear understanding of the institution's mission
- sufficient resources to carry out the mission
- comprehensive institution organization with necessary supporting services
- high quality personnel management structure
- careful matching of institution (layout, design, age, and maintenance) with the type of inmate and a specific staffing level
- appropriate equipment
- programs that enhance security by involving inmates in productive activities

Maintaining security is a continuous process. It demands the efforts of sufficient numbers of staff who are:

- qualified,
- properly trained,
- directed by policies and procedures, and
- supervised
- properly deployed (at the right place, at the right time)

Sound security practices make proper use of available technology while also recognizing the imitations of technology.

This document addresses operational, physical, and technological dimensions of jails, providing the starting point for the identification of potential vulnerabilities.

This document was initially developed as a stand-alone resource for managers. It has been incorporated as Appendix D of the broader *NIC Jail Vulnerability Handbook,* although it may be used separately as needed.

C. How to Use This Manual

This Manual has been developed for use in jails. It is intended to be used by correctional staff and administrators.

Section I (Introduction) provides a brief description of the purpose and scope of this document, and outlines some fundamental security principles.

Section II (Practices) is the heart of the document, and of the vulnerability assessment process. It describes specific activities, or "practices," that should be implemented to maintain facility security. These practices are described in three categories:

A. Operations
B. Equipment and Technical Systems

[1] Henderson, James D., W. Hardy Rauch and Richard L. Phillips, *Guidelines for the Development of a Security Program Second Edition.* Lanham, Maryland. American Correctional Association. 1987

C. Physical Plant

Many of these practices were adapted from the *Fourth Edition Performance Based Standards for Adult Local Detention Facilities (ALDF)*. In the ALDF standards document, each practice is followed by:

* protocols (written documentation that is needed to guide the practice); and

* process indicators (ways to determine if the practices are being properly implemented)

The practices in Section II are presented again in a checklist format in Section III. This provides a tool for systematically applying the practices to the jail setting.

Section IV provides a management tool, in the form of a series of checklists that assemble the activities prescribed in the practices (Section II) according to frequency (by shift, daily, weekly, etc.)

= = = = = = = = = = = =

II: PRACTICES

A. OPERATIONS

A1. STAFFING

A1-1 A comprehensive staffing analysis identifies all posts and positions that are required:

a) to maintain security;
b) observe and supervise inmates and inmate-occupied areas, and
c) respond to emergencies.

A1-2 The facility can document that the overall vacancy rate among the staff positions authorized to work directly with inmates does not exceed 10 percent for any 18-month period.

A1-3 An analysis of daily staff rosters identifies discrepancies between actual practices and staffing plans, to ensure that institutional security is not jeopardized.

A2. INMATE ACCOUNTABILITY

A2-1 COUNTS.

a. There are at least five official counts conducted during each 24-hour period.
b. Counts are conducted by two facility personnel and their counts are compared to ensure they achieve identical results.
c. In areas where inmates are not secured in a cell, one staff member conducts the count while the second ensures there is no inmate movement. Facility personnel then switch positions and conduct a second count.
d. At a minimum, one official count requires inmates to be standing in their cells during the count.
e. During counting, staff are required to see "flesh."
f. Official count slips are signed by all facility personnel who conducted the count for their respective area.
g. Supervisory personnel personally receive the count in the control center once during their shift if a count is conducted.
h. After two inaccurate counts are conducted in a specific area, a picture card count is conducted under the direction of a supervisor to determine the cause of the inaccurate count.
i. Official count documentation is retained for a designated period, but not less than 30 days.

A2-2 CENSUS ACCOUNTABILITY CHECKS. Census accountability checks are conducted in all areas of the facility on a scheduled basis, to determine if all inmates are accounted for and are in their assigned area. The following practices are implemented:

a. Each established inmate or program detail within the facility possesses information to identify each inmate, that includes each assigned inmate's picture, housing unit assignment, custody level and sentence/offense information.

b. An accountability check is conducted each morning of all inmate details and inmates remaining in the housing unit. A second accountability check is conducted after all inmates return to their assigned details after the noon meal. The results of all accountability checks are reported to the control center.
c. Supervisory personnel conduct impromptu accountability checks in all areas of the facility to ensure assigned inmates are present and/or accounted for. At least one check will be conducted each week, involving at least 10% of the program/work assignments.
d. Supervisory personnel conduct a total lock-down accountability check of the facility at a minimum of once a month, to ensure all inmates are in their assigned area.

A2-3 CONTROLLED MOVEMENT.
a. All inmate movement is controlled.
b. Time frames are established for all inmate movement.
c. Maximum staff visibility is provided during inmate movement.

A2-4 IDENTIFICATION. Each inmate is provided with some form of official identification.

A3. EMERGENCY PREPAREDNESS

A3-1 Emergency preparedness plans are reviewed at least annually to ensure the following steps are outlined in response to an inmate escape. Plans for inmate escape address, at a minimum:

a. Staff responsibilities when they become aware of an attempted or successful escape.
b. The use of deadly force.
c. A formalized plan for a quick response/apprehension team and location of weapons for immediate issue.
d. Escape post(s) are pre-designated and cover the immediate area around the facility and include extended posts from the facility.
e. Provisions for quick issuance of weapons.
f. Memoranda of understanding are established with local, state and federal law enforcement officials.

A3-2 The steps necessary to conduct a complete internal search of the facility are described. Plans for internal searches contain, at a minimum:

a. A list of all facility areas.
b. A list of all necessary equipment and/or tools necessary to conduct a thorough search.
c. A list of the number of staff required to search each area identified in the plan.
d. A list of the necessary keys to gain entry to the area.
e. Building diagrams of each area.
f. A check-off sheet to determine which areas have been searched.
g. Provisions for review and revision of the plan at least every 12 months.

A3-3 Emergency Preparedness Drills**:**
a. Staff are familiar with their responsibilities in the event of an emergency.
b. Emergency preparedness drills are conducted at least quarterly and there is a drill for every plan at least once every 12 months.
c. Various scenarios are scripted for emergency preparedness drills.

d. An emergency preparedness drill is conducted with outside law enforcement agencies at least every 12 months to evaluate the memorandum of understanding.
e. Senior administrators of the facility critique each emergency preparedness drill to determine if staff responded in a timely manner and according to facility emergency preparedness plans, and emergency plans are revised when drill critiques indicate that a change is necessary.
f. The results of drills are documented.

A4. INTELLIGENCE

A4-1 A staff member(s) is assigned responsibility for gathering and compiling information regarding criminal activities occurring within and outside of the facility.

A4-2 All telephone calls made by the inmate population are taped and monitored to gather vital information about illegal activities, consistent with applicable laws.

A4-3 Staff maintain a list of inmates who are known escape risks.

A4-4 Inmate mail is monitored as a source of intelligence.

A4-5 Inmate visitation activities are monitored as a source of intelligence, with special instructions regarding inmates on the hot list.

A4-6 Inmate associates are monitored to detect illegal activities.

A4-7 Staff develop and maintain an inmate intelligence-gathering system.

A4-8 DISSEMINATION. Intelligence-gathering staff meet weekly with facility administrators to discuss inmates who are believed to be involved in illegal activities, review the list of known escape risks, and discuss strategies.

A4-9 The facility administrator designates a staff member to act as a liaison between local, state, and federal law enforcement agencies.

A4-10 CLASSIFICATION SYSTEM. There is a formal classification process for managing and separating inmates and administering the facility.

A5. SEARCHES

A5-1 There is a plan that describes procedures for periodic searches of the facility, cells, inmates, visitors, and vehicles. The plan includes provisions for random and unannounced searches.

A5-2 All areas of the facility are searched by respective departmental personnel at least weekly.

A5-3 Security personnel periodically conduct departmental searches and document each area searched, the date and the results.

A5-4 Recreation yards are searched before opening and after closing.

A5-5 Inmates are frequently pat searched throughout the facility to detect and deter the movement of contraband.

A5-6 Consistent with applicable law, inmates are visually strip-searched when necessary.

A6. VISITING

A6-1 PROCESSING INMATE VISITORS. Prior to being admitted into the security perimeter, inmate visitors:

a. Are subjected to an NCIC inquiry to determine their suitability to visit.
b. Are advised of the list of authorized items permitting in the visiting area.
c. Are advised that they are subject to a search of their person and property.
d. Provide a government-issued photo identification.
e. Are on the inmate's pre-approved visiting list.
f. Successfully pass through a metal detector.
g. Sign a log book with name, address, phone number, license plate number and signature.
h. Are under constant supervision while being escorted to the visiting room.
i. Affirm and sign a form that they do not possess any weapons, narcotics, or any other type of contraband.

A6-2 There is a record retention schedule for visiting records and related documentation.

A6-3 PROCESSING INMATES INTO THE VISITING ROOM. The following practices are implemented:

a. All inmates are identified by a facility photograph and prison number prior to admittance.
b. All inmates are visually strip-searched prior to entry into the visiting room and after the completion of their visit.
c. Inmates are under constant supervision while in the visiting room and are under direct staff supervision when bathroom facilities are utilized.
d. Visitors and inmates have separate bathroom facilities.

A6-4 PROCESSING INMATES AND VISITORS AT THE COMPLETION OF VISITING.

a. At the completion of the visit, the inmate and visitor are physically separated and the inmate is identified using a photo ID prior to allowing his/her visitor to leave the visiting room.
b. At the completion of the visiting period, when multiple visitors and inmates are exiting, inmates and visitors are separated into two groups. Inmates are counted and identified using photo ID prior to allowing visitors to leave the visiting room.
c. Visitors are required to sign out of the facility and their signatures are compared to their incoming signatures.
d. The visiting room is searched for contraband after all visitors and inmates have departed.

A7. TRANSPORTATION OF INMATES (Escorted Trips)

A7-1 Inmates do not have prior knowledge of the date, time, and destination of an escorted trip outside of the secure perimeter.

A7-2 Escorting staff review security information on the inmate to familiarize themselves with his/her security risks.

A7-3 Inmates are visually strip searched, scanned with an electronic detection system, and issued clothing which was not available to the inmates prior to the escorted trip.

A7-4 Restraint equipment is applied consistent with the inmates custody level.

A7-5 The escort vehicle is searched for contraband prior to placing the inmate in the vehicle

A7-6 A secure escort vehicle with a separation barrier between staff and the inmate is utilized

A7-7 The number of escort staff are assigned consistent with inmate(s) custody level.

A7-8 Escorting staff contact the institution every 30 minutes and inform them of their status.

A7-9 The inmate is under continuous supervision when escorted outside the secure perimeter.

A7-10 Restraints and escort requirements are not altered without authorization from senior jail personnel.

A7-11 Escorting staff are armed with weapons consistent with facility requirements.

A7-12 Escorting staff qualify at a minimum semi-annually with all weapons utilized when escorting inmates outside the secure perimeter.

A7-13 The institution has a trained cadre of officers and supervisors to conduct escorts outside the secure perimeter.

A7-14 Alternate routes are utilized when escorting inmates to routine areas in the community.

A7-15 Local law enforcement are notified of scheduled and emergency escorted trips into the community.

A7-16 Inmates are visually strip searched and scanned with an electronic detection system when they return to the institution.

A8. SECURITY INSPECTIONS

A8-1 A comprehensive security inspection program includes at a minimum:

a. A list of all areas of the facility to be inspected on a scheduled basis to include each shift, daily, weekly and monthly responsibilities. (see Physical Protection System checklists in Appendix C)
b. A list of all items to be inspected in each designated areas (e.g. doors, locks, security bars, plumbing accesses, windows, etc.)
c. Weekly "tapping" of security bars to ensure no tampering has occurred.
d. A detailed form for each area of the facility that outlines all the requirements, and that provides a space for date and signature.

e. Inspection of tunnels, utility chases, drainage pipes, roofs and manhole covers.
f. Discrepancies discovered during an inspection are reported and corrected in a timely manner.
g. Responsibility for oversight of the security inspection program is assigned to supervisory personnel to ensure compliance.

A9. TRAINING

A9-1 Staff have the knowledge, skills and abilities to perform all assigned duties.

A9-2 There is a training plan that annually addresses, at a minimum: security inspections, tool control, inmate accountability, emergency preparedness, key control, entrance procedures, supervising inmates, firearm's qualification and search procedures.

A9-3 Staff training is documented.

B. EQUIPMENT AND TECHNICAL SYSTEMS

SECURITY-RELATED TECHNOLOGY

B1. Video Systems

B1-1 All cameras and installations are accurately described, using Checklist B4
[Appendix B Checklist 4, Video System Inventory]

B1-2 Video equipment is installed according to manufacturers' specifications.

B1-3 Video equipment is maintained, inspected, and tested according to manufacturers' specifications.

B1-4 Problems with video systems and equipment are promptly identified and are corrected as soon as possible. Priority is assigned to the repair of systems/equipment that are of most importance for facility security. Repairs are documented.

B1-5 There are maintenance agreements for the repair of security systems. Emergency service and repair numbers are available to staff to be used when needed.

B1-6 Assigned staff use security systems properly and understand the capabilities of the technology.

B1-7 Staff are provided in sufficient numbers to view monitors.

B1-8 Staff verify that video equipment is operational at least once on each shift.

B1-9 Video surveillance equipment enhances perimeter security and the following requirements are met, at a minimum:

a. All cameras installed to monitor the secure perimeter are reviewed to determine if placement is consistent with the capabilities of the cameras(i.e. various lighting situations, fixed versus zoom.)
b. The number of cameras installed is reviewed to determine if there are sufficient cameras to monitor the secure perimeter.
c. The placement of cameras is reviewed to determine if the field of surveillance is overlapping.
d. Maintenance records are reviewed to determine if the surveillance equipment is maintained according to manufactures' specification.
e. Maintenance records are reviewed to determine if surveillance equipment is repaired when malfunctions are reported.

B2. Alarm and Sensor Systems (If used)

B2-1 All alarm and sensor equipment is accurately described, using Checklist B5, Appendix B.)

B2-2 There is documentation from a certified independent authority that alarm and sensor equipment is installed according to manufacturers' specifications.

B2-3 Alarm and sensor equipment is maintained, inspected, and tested according to manufacturers' specifications.

B2-4 Problems with alarm and sensor systems and equipment are promptly identified and are corrected as soon as possible. Priority is assigned to the repair of systems/equipment that are of most importance for facility security. Repairs are documented.

B2-5 There are maintenance agreements for the repair of alarm and sensor systems. Emergency service and repair numbers are available to staff to be used when needed.

B2-6 Assigned staff properly use alarm and sensor systems and understand the capabilities of the technology.

B2-7 Staff check fence alarm and sensor systems at least daily by triggering the alarm in each zone.

B3. Metal and Other Detectors

B3-1 Metal detectors are strategically placed throughout the facility to enhance searches.

B3-2 Walk-through metal detectors are will be checked daily by supervisory personnel to ensure they are operational. The results of these checks are recorded.

B3-3 All metal and other detection equipment is accurately described, using Checklist B6, Appendix B.

B3-4 There is documentation from a certified independent authority that metal and other detection equipment is installed according to manufacturers' specifications.

B3-5 Metal and other detection equipment is maintained, inspected, and tested according to manufacturers' specifications.

B3-6 Problems with metal and other detection equipment are promptly identified and are corrected as soon as possible. Priority is assigned to the repair of systems/equipment that are of most importance for facility security. Repairs are documented.

B3-7 There are maintenance agreements for the repair of metal and other detection equipment. Emergency service and repair numbers are available to staff to be used when needed.

B3-8 Assigned staff properly use metal and other detection equipment and understand the capabilities of the technology.

B4. PHYSICAL PLANT SECURITY

B4-1 A thorough self-analysis is conducted at least annually to identify potential threats for all areas of the facility and to determine potential vulnerabilities from internal and outside threats that could breach the secure perimeter and/or interrupt vital services. This analysis is re-examined whenever there is a substantial change in the physical plant or in the security requirements of the inmate population.

B4-2 The threat analysis, at a minimum:

a. Identifies the full range of threats that could result in an inmate escape or other threat.
b. Examines each type of threat.
c. Explores contingencies associated with each type of threat.
d. Develops scenarios that describe specific responses to each type of threat.
e. Evaluates each scenario to determine if responses are feasible.

B4-3 Physical and operational deficiencies identified in the threat analysis are corrected in a timely manner.

B5. PERIMETER SECURITY

Perimeter Fence (If applicable)

B5-1 Perimeter fences equipped with alarm systems are inspected and tested on a pre-established schedule, to include at a minimum:

a. Staff responsible for monitoring the fence alarm system ensure the system is tested at the control panel at the beginning of each shift.

b. The fence is inspected each shift to ensure no tampering has occurred.
c. Security personnel test the alarm system at least once daily by physically activating each zone.
d. All alarms are promptly investigated and documented.
e. Alarm documentation is reviewed by supervisory personnel to determine if the alarm system is frequently or infrequently shut off in specific zones without written supervisory authorization.
f. When there is a false alarm, the cause is identified and, if necessary, repaired.
g. If the alarm system provides a computerized printout of all activity, supervisory personnel review this printout to determine the integrity of the system.

Communication Capabilities (If applicable)

B5-2 All perimeter posts are able to communicate with each other and with the facility control center at all times, without interference or interruptions.

Fixed Perimeter Posts (If applicable)

B5-3 All fixed perimeter posts have overlapping supervision of all areas within the secure perimeter.

B5-4 All weapons assigned to a fixed perimeter post meet the following minimum requirements:

a. The types of weapons assigned to a fixed perimeter post have been reviewed to determine their suitability for task requirements such as range and accuracy for potential targets.
b. Weapons assigned to a fixed perimeter post are cleaned on a scheduled basis.
c. Ammunition and weapons are exchanged on at least a quarterly basis.

B5-5 Facility personnel assigned to a fixed perimeter post qualify every 12 months with all assigned weapons.

B5-6 Facility personnel assigned to a fixed perimeter post receive quarterly re-familiarization training on all weapons associated with the post.

B5-7 Supervisory staff inspect all fixed perimeter posts at least weekly to determine if equipment is maintained in good working order and staff are familiar with their responsibilities.

B5-8 Supervisory staff question personnel assigned to fixed perimeter posts regarding their knowledge of the policy regarding use of deadly force.

B5-9 A maintenance program addresses all functions of perimeter patrol vehicles.

Tunnels and Draining Pipes

B5-10 All tunnels, and drainage pipes that cross the secure perimeter are equipped with security bars.

B6. LOCKING SYSTEMS (KEY/LOCK CONTROL)

B6-1 There is a comprehensive key control program.

B6-2 All locking devices will be reviewed to determine if they are appropriate for the facility.

B6-3 All locking mechanisms are maintained according to manufacturer's specifications.

B6-4 All key rings and keys are counted on a Master Inventory on a daily basis by the Control Center staff.

B6-5 A master inventory in the lock shop lists all keys for each area, make of lock, facility identification number and back-up keys.

B6-6 There are emergency key rings for all areas and these are kept separately from general issue keys.

B6-7 The issuance of key rings is broken down into the following categories: general issue for all staff; issue to individuals in a respective department; restricted key rings requiring supervisory authorization; and emergency key rings.

B6-8 There is no "Master Key" system.

B6-9 When security keys are lost or misplaced, supervisory personnel are notified verbally, immediately followed by a written report. Replacement locks are installed or the locks are re-keyed.

B6-10 Inmates are never permitted to possess keys.

B6-11 Keys are only issued to authorized personnel using a sign out or chit system, or a similar system for accountability purposes.

B6-12 Backup key rings are maintained in at least one alternative location, outside of the facility, to provide emergency response teams with the ability to enter and move within the institution without detection, when necessary.

B6-13 Key rings are assigned a key ring number and the number of keys on each key ring are indicated.

B6-14 All key rings issued to staff are equipped with a security key chain to prevent rings from being dropped, lost or misplaced.

B6-15 Keys are only removed from a key ring by authorized personnel.

B6-16 Security keys are never removed from facility property.

B6-17 The facility has access to a locksmith.

B6-18 Whenever possible, all security keys have a key cut cover.

B7. CONTROL CENTER

B7-1 Control centers, at a minimum:

a. Are constructed to be impervious to unauthorized entry.
b. Are equipped with sallyport entry doors.
c. Have an exterior door that is electrically controlled by control center personnel.
d. Are staffed by qualified correctional personnel.

B7-2 Control center staff identify all facility personnel, visitors and inmates prior to allowing them to enter or depart through their area of supervision.

B7-3 All security doors, grilles and gates controlled by the control center have camera monitoring capabilities or can be viewed directly so that persons are identified before doors are opened.

B8. TOOL CONTROL

B8-1 A facility tool control program covers all applicable areas and is reviewed at least quarterly for compliance.

B8-2 A staff member is designated as facility Tool Control Officer, and is responsible for all aspects of the tool control program.

B8-3 All tools maintained by a facility will be classified as either Hazardous (present an inherent security risk such as hacksaw blades, cutting torches, ladders and rivet guns) or Non-Hazardous (present a lower level of risk and include such items as wrenches, pliers, and screwdrivers.)

B8-4 A tool inventory program includes at a minimum:

a. A designated staff member is assigned responsibility for maintaining the tool inventories throughout the facility.
b. All tools maintained in the facility are kept on a Master Tool Inventory either by log book, bin card system or on a computer-based format.
c. All departments that maintain tools have an identical tool inventory posted with the tools and all tools are accounted for daily.
d. The department identification codes are listed on all tool inventories.

e. Tool inventories are conducted by supervisory staff at least quarterly.
f. Tool inventories are re-issued on an annual basis at a designated time.

B8-5 A system documents the issuance of tools to ensure accountability.

B8-6 Hazardous tools are only issued to staff for their use, or for use by inmates under the direct supervision of staff.

B8-7 The following apply to the acquisition of tools:

a. When tools are purchased, they are received by the facility Tool Control Officer.
b. Tool purchase order copies are provided to the Tool Control Officer.
c. All tools are etched with departmental identification codes before issuance.
d. The master and departmental tool inventories are updated whenever new tools are issued to a department.

B8-8 Tool storage practices at a minimum comply with the following:

a. Hazardous tools are stored in a reinforced concrete room with a security key locking system.
b. Non-hazardous tools are stored in either a secure room with one security key locking system or a secure wire mesh cage with a padlock.
c. In each location where tools are stored, there are “Shadow Boards” that have a light-colored background with a dark outline of each tool painted on it that facilitates instant identification of a missing tool. The color of the dark outline corresponds to the level of classification of the tool.
d. If boxes of tools are assigned to areas in the facility, each box is clearly identified as belonging in the area to which it is assigned. Inside each box is an inventory list of all authorized tools.

B8-9 When a tool is broken or worn out, the facility Tool Control Officer is responsible for documenting the destruction of the tool and revising the master and departmental tool inventories.

B8-10 All tools brought into the facility on a temporary basis by either a vendor or contractor are inventoried prior to entering the secure perimeter.

B8-11 Vendors and contractors are under direct supervision by facility personnel while in the secure perimeter.

B8-12 All tools are re-inventoried before the vendor or contractor is allowed to leave the secure perimeter.

B8-13 A quarterly audit of all tool control practices is conducted by a supervisory staff member.

B9. UTILITIES AND MECHANICAL SYSTEMS

B9-1 Staff are able to communicate with each other and the facility control center without interference or interruptions at all times.

B9-2 Inmates are under direct supervision whenever they are allowed to work on facility telephone and other communications systems. Inmates never have access to two-way communications equipment such as radios.

B9-3 An emergency lighting system provides illumination for critical areas of the facility in the event of a power failure.

B9-4 All spaces in which mechanical systems are located are secured from unauthorized access.

B10. TOXIC/CAUSTICS CONTROL

B10-1 Material Safety Data Sheets are available to identify all toxic, caustic and flammable materials maintained in the facility.

B10-2 All toxic, caustic and flammable materials are:

a. Inventoried, and access to them is controlled.
b. Safely stored in appropriate containers and clearly labeled.
c. Utilized under staff supervision.
d. Disposed of in a manner consistent with Material Safety Data Sheets, and the disposal is documented.

C. PHYSICAL PLANT

C1. LOCATION AND SITE

C1-1 Inventory forms B1 and B2 are completed (Appendix B).

C1-2 Inventory forms B1 and B2 are analyzed to identify escape risks posed by: proximity and adjacencies; visibility and observation; continuity; and condition. (See directions in Appendix B) Findings are clearly documented.

C1-3 The risks identified in C1-2 above are analyzed and, where possible, remedial steps are taken to reduce risks.

C2. FACILITY DESIGN/LAYOUT and BUILDING CONSTRUCTION

C2-1 Inventory forms B3 and B4 are completed (Appendix B).

C1-2 Inventory forms B3 and B4 are analyzed to identify escape risks posed by: proximity and adjacencies; visibility and observation; continuity; and condition. (See directions in Appendix B) Findings are clearly documented.

C1-3 The risks identified in C2-2 above are analyzed and, where possible, remedial steps are taken to reduce risks.

C3 ENTRANCES AND EXITS IN THE SECURE PERIMETER

C3-1 Whenever there is an opening in the security perimeter, there are at least two interlocked doors or gates that create a secure "sallyport." The gates/doors have an interlock system that allow only one gate or door to be opened at a time. All vehicle gates and sallyport doors are equipped with a manual override system in case of a power outage.

C3-2 All sallyport doors are controlled from a secure area where inmates and the public have no access.

C3-3 All persons and vehicles are thoroughly searched prior to allowing entry or exit from the secure perimeter.

Institutional Visitors

C3-4 All institutional visitors are screened before being allowed entry to the secure perimeter. Visitors entering the secure perimeter are:

a. The subject of an NCIC inquiry to determine their suitability for visiting.
b. Asked to disclose the purpose of their visit.
c. Asked if they possess any firearms, ammunition, narcotics, and other contraband items.
d. Required to sign in and to affirm in writing that they possess no contraband.
e. Required to present one form of photo identification.
f. Scanned with a metal detector.

C3-5 A visitor's log is utilized for each visitor to enter name, date, time of visit, purpose of visit and departure time from the secure perimeter. The period of retention for this log is established.

C3-6 Institutional visitors are under direct supervision by facility personnel while inside the secure perimeter. Exceptions must be approved by the warden or designee.

C3-7 The facility uses at least two means of identifying visitors before each visitor exits the secure perimeter.

Vehicles

C3-8 No vehicle is left unattended while in the secure perimeter unless it has been disabled.

C3-9 All civilian drivers are required to stay inside their vehicle while in the secure perimeter. If it is necessary for them to exit the vehicle, the cab is secured and the keys are retained by escorting personnel.

C3-10 No civilian vendor with a split delivery load is allowed access to the secure perimeter.

C3-11 Staff responsible for escorting vehicles inside the secure perimeter do so in such a manner that it allows him/her maximum supervision over the vehicle.

C3-12 Any vehicle that cannot be thoroughly searched prior to exiting the facility must remain inside the secure facility through at least two official counts. Any vehicle that remains inside the secure perimeter overnight must be rendered inoperable and enhanced security measures are employed.

C3-13 Enhanced security measures, such as closing inmates access to an area, are made whenever a concrete truck or a truck that has hydraulic lift or crane capabilities is allowed inside the secure perimeter.

C3-14 Interior and exterior vehicle gates are equipped with crash barriers that are designed to prevent large trucks from compromising the secure perimeter.

C3-15 All inmates entering or exiting the secure perimeter entrances are positively identified, visually searched, scanned electronically, and a record is maintained of each inmate's name, number, date, time in and out.

C3-16 There is a duress code that ensures staff in the vehicle gate are not under duress when requesting a vehicle gate to be opened.

<u>C4. ARMORY</u>

C4-1 The facility maintains an armory with emergency equipment to respond to emergencies and security threats. Armories are located to address internal and external threats.

C4-2 Armories are constructed to prevent unauthorized entry.

C4-3 Armories are constructed with a sallyport entry way that is electrically controlled from a remote secure location that has camera monitoring capabilities.

C4-4 The armory has limited access.

C4-5 A quarterly inventory all weapons and ammunition is conducted.

<u>C5. MAIL ROOM</u>

C5-1 The following practices are employed to prevent the introduction of contraband:

a. All packages are opened and inspected for contraband prior to entering the secure perimeter.

b. All mail bags and packages are searched via electronic equipment for the concealment of contraband prior to entering the secure perimeter.
c. All outgoing letters are screened for possible illegal activity.
d. All incoming first class mail are physically searched by mail room personnel prior to distribution.

C5-2 Staff are trained to identify threats that are posed by facility mail. The facility uses resources available from the U.S. Postal Service to enhance staff training and facility safety.

C6. TRASH COLLECTION/DISPOSAL

C6-1 TRASH TRUCKS.

a. If trash trucks are attended by inmates, they are classified as minimum security.
b. Compacting controls on each truck are operated by facility personnel.
c. Trash collection and operation of the vehicle are under constant facility personnel supervision.
d. Trash trucks are rendered inoperable until removed from the secure perimeter.
e. Trash trucks are left in a secure location through two official counts prior to being allowed to leave the secure perimeter.

C6-2 TRASH COMPACTOR.

a. Keys for the trash compactor are classified as restricted keys and are controlled by staff.
b. Compacting controls are only operated by facility personnel.
c. Facility personnel conduct an inmate count of the trash detail prior to, and upon completion of, the trash compacting process.
d. Facility personnel responsible for the trash compactor detail maintain control over the trash compactor area during the compacting process.
e. The trash compactor and controls are locked when not in use.
f. Prior to removing the trash compactor from the secure perimeter, it is relocated to a secure location where enhanced security measures are implemented, and remains in the secure location for a least two official counts prior to being removed from the secure perimeter.

= = = = = = = = = = =

III. Practices and Protocols Checklist

Ratings: Superior, **G**ood, **A**cceptable, **M**arginal, **A**t Risk

Practices	Findings S,G,A,M,A	Comments
<u>A. OPERATIONS</u> **<u>A1. STAFFING</u>** **A1-1** A comprehensive staffing analysis identifies all posts and positions that are required: a. to maintain security;		
b. observe and supervise inmates and inmate-occupied areas, and		
c. respond to emergencies.		
A1-2 The facility can document that the overall vacancy rate among the staff positions authorized to work directly with inmates does not exceed 10 percent for any 18-month period.		
A1-3 An analysis of daily staff rosters identifies discrepancies between actual practices and staffing plans, to ensure that institutional security is not jeopardized.		
<u>A2. INMATE ACCOUNTABILITY</u> **A2-1** COUNTS. a. There are at least five official counts conducted during each 24-hour period.		
b. All areas conducting a count are counted by two facility personnel and their counts compared to ensure they achieve identical results.		
c. In areas where inmates are not secured in a cell, one staff member conducts the count while the second ensures there is no inmate movement. Facility personnel then switch positions and conduct a second count.		
d. At a minimum, one official count requires inmates to be standing in their cells during the count.		
e. During counting, staff are required to see “flesh.”		
f. Official count slips are signed by all facility personnel who conducted the count for their respective area.		
g. Supervisory personnel personally receive the count in the control center once during their shift if a count is conducted.		
h. After two inaccurate counts are conducted in a specific area, a picture card count is conducted under the direction of a supervisor to determine the cause of the inaccurate count.		
i. Official count documentation is retained for a designated period, but not less than 30 days.		
A2-2 CENSUS ACCOUNTABILITY CHECKS. Census accountability checks are conducted in all areas of the facility on a scheduled basis, to determine if all inmates are accounted for and are in their assigned area. The following practices are implemented:		
a. Each established inmate or program detail within the facility possesses information to identify each inmate, that includes each assigned inmate's picture, housing unit assignment, custody level and sentence/offense information.		

b. An accountability check is conducted each morning of all inmate details and inmates remaining in the housing unit. A second accountability check is conducted after all inmates return to their assigned details after the noon meal. The results of all accountability checks are reported to the control center.		
c. Supervisory personnel conduct impromptu accountability checks in all areas of the facility to ensure assigned inmates are present and/or accounted for. At least one check will be conducted each week, involving at least 10% of the program/work assignments.		
d. Supervisory personnel conduct a total lock-down accountability check of the facility at a minimum of once a month, to ensure all inmates are in their assigned area.		
A2-3 CONTROLLED MOVEMENT. a. All inmate movement is controlled.		
b. Time frames are established for all inmate movement.		
c. Maximum staff visibility is provided during inmate movement.		
A2-4 IDENTIFICATION. Each inmate is provided with some form of official identification.		
<u>A3. EMERGENCY PREPAREDNESS</u> **A3-1** Emergency preparedness plans are reviewed annually to ensure the following steps are outlined in response to an inmate escape. Plans for inmate escape contain, at a minimum:		
a. Staff responsibilities when they become aware of an attempted or successful escape.		
b. The use of deadly force.		
c. A formalized plan for a quick response/apprehension team and location of weapons for immediate issue.		
d. Escape post(s) are pre-designated and cover the immediate area around the facility and include extended posts from the facility.		
e. There are provisions for quick issuance of weapons.		
f. Memoranda of understanding are established with local, state and federal law enforcement officials.		
A3-2 The steps necessary to conduct a complete internal search of the facility are described. Plans for internal searches contain, at a minimum: a. A list of all facility areas.		
b. A list of all necessary equipment and/or tools necessary to conduct a thorough search.		
c. A list of the number of staff required to search each area identified in the plan.		
d. A list of the necessary keys to gain entry to the area.		
e. Individual building diagrams of each area.		
f. A check-off sheet to determine which areas have been searched.		
g. Provisions for review and revision of the plan at least every 12 months.		
A3-3 <u>Emergency Preparedness Drills</u>**:** a. Staff are familiar with their responsibilities in the event of an emergency.		

b. Emergency preparedness drills are conducted at least quarterly and there is a drill for every plan at least once every 12 months.		
c. Various scenarios are scripted for emergency preparedness drills.		
d. An emergency preparedness drill is conducted with outside law enforcement agencies at least every 12 months to evaluate the memorandum of understanding.		
e. Senior administrators of the facility critique each emergency preparedness drill to determine if staff responded in a timely manner and according to facility emergency preparedness plans, and emergency plans are revised when drill critiques indicate that a change is necessary.		
f. The results of drills are documented.		
A4. INTELLIGENCE **A4-1** A staff member(s) is assigned responsibility for gathering and compiling information regarding criminal activities occurring within and outside of the facility.		
A4-2 All telephone calls made by the inmate population are taped and monitored to gather vital information about illegal activities, consistent with applicable laws.		
A4-3 Staff maintain a list of inmates who are known escape risks.		
A4-4 Inmate mail is monitored as a source of intelligence.		
A4-5 Inmate visitation activities are monitored as a source of intelligence, with special instructions regarding inmates on the hot list.		
A4-6 Inmate associates are monitored to detect illegal activities.		
A4-7 Staff develop and maintain an inmate intelligence-gathering system.		
A4-8 DISSEMINATION. Intelligence-gathering staff meet weekly with facility administrators to discuss inmates who are believed to be involved in illegal activities, review the list of known escape risks, and discuss strategies.		
A4-9 The facility administrator designates a staff member to act as a liaison between local, state, and federal law enforcement agencies.		
A4-10 CLASSIFICATION SYSTEM. There is a formal classification process for managing and separating inmates and administering the facility.		
A5. SEARCHES **A5-1** There is a plan that describes procedures for periodic searches of the facility, cells, inmates, visitors, and vehicles. The plan includes provisions for random and unannounced searches.		
A5-2 All areas of the facility are searched by respective departmental personnel at least weekly.		
A5-3 Security personnel periodically conduct departmental searches and document each area searched, the date and the results.		
A5-4 Recreation yards are searched before opening and after closing.		

A5-5 Inmates are frequently pat searched throughout the facility to detect and deter the movement of contraband.		
A5-6 Consistent with applicable law, inmates are visually strip-searched when necessary.		
<u>A6. VISITING</u> **A6-1** PROCESSING INMATE VISITORS. Prior to being admitted into the security perimeter, inmate visitors: a. are subjected to an NCIC inquiry to determine their suitability to visit.		
b. are advised of the list of authorized items permitting in the visiting area.		
c. are advised that they are subject to a search of their person and property.		
d. provide a government-issued photo identification.		
e. are on the inmate's pre-approved visiting list.		
f. successfully pass through a metal detector.		
g. sign a log book with name, address, phone number, license plate number and signature.		
h. are under constant supervision while being escorted to the visiting room.		
i. affirm and sign a form that they do not possess any weapons, narcotics, or any other type of contraband.		
A6-2 There is a record retention schedule for visiting records and related documentation.		
A6-3 PROCESSING INMATES INTO THE VISITING ROOM. The following practices are implemented: a. All inmates are identified by a facility photograph and prison number prior to admittance.		
b. All inmates are visually strip-searched prior to entry into the visiting room and after the completion of their visit.		
c. Inmates are under constant supervision while in the visiting room and are under direct staff supervision when bathroom facilities are utilized.		
d. Visitors and inmates have separate bathroom facilities.		
A6-4 PROCESSING INMATES AND VISITORS AT THE COMPLETION OF VISITING. a. At the completion of the visit, the inmate and visitor are physically separated and the inmate is identified using a photo ID prior to allowing his/her visitor to leave the visiting room.		
b. At the completion of the visiting period, when multiple visitors and inmates are exiting, inmates and visitors are separated into two groups. Inmates are counted and identified using photo ID prior to allowing visitors to leave the visiting room.		
c. Visitors are required to sign out of the facility and their signatures are compared to their incoming signatures.		
d. The visiting room is searched for contraband after all visitors and inmates have departed.		
<u>A7. TRANSPORTATION OF INMATES (Escorted Trips)</u> **A7-1** Inmates do not have prior knowledge of the date, time, and destination of an escorted trip outside of the secure perimeter.		

A7-2 Escorting staff review security information on the inmate to familiarize themselves with his/her security risks.		
A7-3 Inmates are visually strip searched, scanned with an electronic detection system, and issued clothing which not available to the inmates prior to the escorted trip.		
A7-4 Restraint equipment is applied consistent with the inmates custody level.		
A7-5 The escort vehicle is searched for contraband prior to placing the inmate in the vehicle		
A7-6 A secure escort vehicle with a separation barrier between staff and the inmate is utilized		
A7-7 Escort staff are assigned consistent with the inmates custody level.		
A7-8 Escorting staff contact the institution every 30 minutes and inform them of their status.		
A7-9 The inmate is under continuous supervision when escorted outside the secure perimeter.		
A7-10 Restraints and escort requirements are not altered without authorization from senior institution personnel.		
A7-11 Escorting staff are armed with weapons consistent with institution requirements.		
A7-12 Escorting staff qualify at a minimum semi-annually with all weapons utilized when escorting inmates outside the secure perimeter.		
A7-13 The institution has a trained cadre of officers and supervisors to conduct armed escorts outside the secure perimeter.		
A7-14 Alternate routes are utilized when escorting inmates to routine areas in the community.		
A7-15 Local law enforcement are notified of scheduled and emergency escorted trips into the community.		
A7-16 Inmates are visually strip searched and scanned with an electronic detection system when they return to the institution.		
<u>**A8. SECURITY INSPECTIONS**</u> **A8-1** A comprehensive security inspection program includes at a minimum: a. A list of all areas of the facility to be inspected on a scheduled basis to include each shift, daily, weekly and monthly responsibilities. (see checklists in Appendix C)		
b. A list of all items to be inspected in each designated areas (e.g. doors, locks, security bars, plumbing accesses, windows, etc.)		
c. Weekly "tapping" of security bars to ensure no tampering has occurred.		
d. A detailed form for each area of the facility that outlines all the requirements, and that provides a space for date and signature.		
e. Inspection of tunnels, utility chases, drainage pipes, roofs and manhole covers.		
f. Discrepancies discovered during an inspection are reported and corrected in a timely manner.		
g. Responsibility for oversight of the security inspection program is assigned to supervisory personnel to ensure compliance.		

A9. TRAINING **A9-1** Staff have the knowledge, skills and abilities to perform all assigned duties.		
A9-2 There is a training plan that annually addresses, at a minimum: security inspections, tool control, inmate accountability, emergency preparedness, key control, entrance procedures, supervising inmates, firearm's qualification and search procedures.		
A9-3 Staff training is documented.		
B. EQUIPMENT AND TECHNICAL SYSTEMS SECURITY-RELATED TECHNOLOGY **B1. Video Systems** **B1-1** All cameras and installations are accurately described, using Checklist B4 [Appendix B Checklist 4, Video System Inventory]		
B1-2 Video equipment is installed according to manufacturers' specifications.		
B1-3 Video equipment is maintained, inspected, and tested according to manufacturers' specifications.		
B1-4 Problems with video systems and equipment are promptly identified and are corrected as soon as possible. Priority is assigned to the repair of systems/equipment that are of most importance for facility security. Repairs are documented.		
B1-5 There are maintenance agreements for the repair of security systems. Emergency service and repair numbers are available to staff to be used when needed.		
B1-6 Assigned staff use security systems properly and understand the capabilities of the technology.		
B1-7 Staff are provided in sufficient numbers to view monitors.		
B1-8 Staff verify that video equipment is operational at least once on each shift.		
B1-9 Video surveillance equipment enhances perimeter security and the following requirements are met, at a minimum: a. All cameras installed to monitor the secure perimeter are reviewed to determine if placement is consistent with the capabilities of the cameras(i.e. various lighting situations, fixed versus zoom.)		
b. The number of cameras installed is reviewed to determine if there are sufficient cameras to monitor the secure perimeter.		
c. The placement of cameras is reviewed to determine if the field of surveillance is overlapping.		
d. Maintenance records are reviewed to determine if the surveillance equipment is maintained according to manufactures' specification.		
e. Maintenance records are reviewed to determine if surveillance equipment is repaired when malfunctions are reported.		
B2. Alarm and Sensor Systems **B2-1** All alarm and sensor equipment is accurately described, using Checklist B5, Appendix B.)		

B2-2 There is documentation from a certified independent authority that alarm and sensor equipment is installed according to manufacturers' specifications.		
B2-3 Alarm and sensor equipment is maintained, inspected, and tested according to manufacturers' specifications.		
B2-4 Problems with alarm and sensor systems and equipment are promptly identified and are corrected as soon as possible. Priority is assigned to the repair of systems/equipment that are of most importance for facility security. Repairs are documented.		
B2-5 There are maintenance agreements for the repair of alarm and sensor systems. Emergency service and repair numbers are available to staff to be used when needed.		
B2-6 Assigned staff properly use alarm and sensor systems and understand the capabilities of the technology.		
B2-7 Staff check fence alarm and sensor systems at least daily by triggering the alarm in each zone.		
B3. Metal and Other Detectors **B3-1** Metal detectors are strategically placed throughout the facility to enhance searches.		
B3-2 Walk through metal detectors are will be checked daily by supervisory personnel to ensure they are operational. The results of these checks are recorded.		
B3-3 All metal and other detection equipment is accurately described, using Checklist B6, Appendix B.		
B3-4 There is documentation from a certified independent authority that metal and other detection equipment is installed according to manufacturers' specifications.		
B3-5 Metal and other detection equipment is maintained, inspected, and tested according to manufacturers' specifications.		
B3-6 Problems with metal and other detection equipment are promptly identified and are corrected as soon as possible. Priority is assigned to the repair of systems/equipment that are of most importance for facility security. Repairs are documented.		
B3-7 There are maintenance agreements for the repair of metal and other detection equipment. Emergency service and repair numbers are available to staff to be used when needed.		
B3-8 Assigned staff properly use metal and other detection equipment and understand the capabilities of the technology.		
B4. PHYSICAL PLANT SECURITY **B4-1** A thorough self-analysis is conducted at least annually to identify potential threats for all areas of the facility and to determine potential vulnerabilities from outside threats that could breach the secure perimeter and/or interrupt vital services. This analysis is re-examined whenever there is a substantial change in the physical plant or in the security requirements of the inmate population.		
B4-2 The threat analysis includes, at a minimum: a. Identifies the full range of threats that could result in an inmate escape.		

b. Examines each type of threat.		
c. Explores contingencies associated with each type of threat.		
d. Develops scenarios that describe specific responses to each type of threat.		
e. Evaluates each scenario to determine if responses are feasible.		
B4-3 Physical and operational deficiencies identified in the threat analysis are corrected in a timely manner.		
B5-1 Perimeter fences equipped with alarm systems are inspected and tested on a pre-established schedule, to include at a minimum: a Staff responsible for monitoring the fence alarm system ensure the system is tested at the control panel at the beginning of each shift.		
b. The fence is inspected each shift to ensure no tampering has occurred.		
c. Security personnel test the alarm system at least once daily by physically activating each zone.		
d. All alarms are promptly investigated and documented.		
e. Alarm documentation is reviewed by supervisory personnel to determine if the alarm system is frequently or infrequently shut off in specific zones without written supervisory authorization.		
f. When there is a false alarm, the cause is identified and, if necessary, repaired.		
g. If the alarm system provides a computerized printout of all activity, supervisory personnel review this printout to determine the integrity of the system.		
<u>Communication Capabilities</u> **B5-2** All perimeter posts are able to communicate with each other and with the facility control center without interference or interruptions at all times.		
<u>Fixed Perimeter Posts</u> **B5-3** All fixed perimeter posts have overlapping supervision of all areas within the secure perimeter.		
B5-4 All weapons assigned to a fixed perimeter post meet the following minimum requirements: a. The types of weapons assigned to a fixed perimeter post have been reviewed to determine their suitability for task requirements such as range and accuracy for potential targets.		
b. Weapons assigned to a fixed perimeter post are cleaned on a scheduled basis.		
c. Ammunition and weapons are exchanged on at least a quarterly basis.		
B5-5 Facility personnel assigned to a fixed perimeter post qualify every 12 months with all assigned weapons.		
B5-6 Facility personnel assigned to a fixed perimeter post receive quarterly re-familiarization training on all weapons associated with the post.		
B5-7 Supervisory staff inspect all fixed perimeter posts at least weekly to determine if equipment is maintained in good working order and staff are familiar with their responsibilities.		

B5-8 Supervisory staff question personnel assigned to fixed perimeter posts regarding their knowledge of the policy regarding use of deadly force.		
B5-9 A maintenance program addresses all functions of perimeter patrol vehicles.		
<u>Tunnels and Draining Pipes</u> **B5-10** All tunnels, and drainage pipes that cross the secure perimeter are equipped with security bars.		
<u>B6. LOCKING SYSTEMS (KEY/LOCK CONTROL)</u> **B6-1** There is a comprehensive key control program.		
B6-2 All locking devices will be reviewed to determine if they are appropriate for the facility.		
B6-3 All locking mechanisms are maintained according to manufacturer's specifications.		
B6-4 All key rings and keys are counted on a Master Inventory on a daily basis by the Control Center staff.		
B6-5 A master inventory in the lock shop lists all keys for each area, make of lock, facility identification number and back-up keys.		
B6-6 There are emergency key rings for all areas and these are kept separately from general issue keys.		
B6-7 The issuance of key rings is broken down into the following categories: general issue for all staff; issue to individuals in a respective department; restricted key rings requiring supervisory authorization; and emergency key rings.		
B6-8 There is no "Master Key" system.		
B6-9 When security keys are lost or misplaced, supervisory personnel are notified verbally, immediately followed by a written report. Replacement locks are installed or the locks are re-keyed.		
B6-10 Inmates are never permitted to possess keys.		
B6-11 Keys are only issued to authorized personnel using a sign out or chit system, or a similar system for accountability purposes.		
B6-12 Backup key rings are maintained in at least one alternative location, outside of the facility, to provide emergency response teams with the ability to enter and move within the institution without detection, when necessary.		
B6-13 Key rings are assigned a key ring number and the number of keys on each key ring are indicated.		
B6-14 All key rings issued to staff are equipped with a security key chain to prevent rings from being dropped, lost or misplaced.		
B6-15 Keys are only removed from a key ring by authorized personnel.		
B6-16 Security keys are never removed from facility property.		
B6-17 The facility has a full-time locksmith to implement and monitor the key control procedures.		
B6-18 Whenever possible, all security keys have a key cut cover.		

B7. CONTROL CENTER **B7-1** Control centers, at a minimum: a. Are constructed to be impervious to unauthorized entry.		
b. Are equipped with sallyport entry doors.		
c. Have an exterior door that is electrically controlled by control center personnel.		
d. Are staffed by qualified correctional personnel.		
B7-2 Control center staff identify all facility personnel, visitors and inmates prior to allowing them to enter or depart through their area of supervision.		
B7-3 All security doors, grilles and gates controlled by the control center have camera monitoring capabilities or can be viewed directly so that persons are identified before doors are opened.		
B8. TOOL CONTROL **B8-1** A facility tool control program covers all applicable areas and is reviewed at least quarterly for compliance.		
B8-2 A staff member is designated as facility Tool Control Officer, and is responsible for all aspects of the tool control program.		
B8-3 All tools maintained by a facility will be classified as either Hazardous (present an inherent security risk such as hacksaw blades, cutting torches, ladders and rivet guns) or Non-Hazardous (present a lower level of risk and include such items as wrenches, pliers, and screwdrivers.)		
B8-4 A tool inventory program includes at a minimum: a. designated staff member is assigned responsibility for maintaining the tool inventories throughout the facility.		
b. All tools maintained in the facility are kept on a Master Tool Inventory either by log book, bin card system or on a computer-based format.		
c. All departments that maintain tools have an identical tool inventory posted with the tools and all tools are accounted for daily.		
d. The department identification codes are listed on all tool inventories.		
e. dTool inventories are conducted by supervisory staff at least quarterly.		
f. Tool inventories are re-issued on an annual basis at a designated time.		
B8-5 A system documents the issuance of tools to ensure accountability.		
B8-6 Hazardous tools are only issued to staff for their use, or for use by inmates under the direct supervision of staff.		
B8-7 The following apply to the acquisition of tools: a. When tools are purchased, they are received by the facility Tool Control Officer.		
b. Tool purchase order copies are provided to the Tool Control Officer and the facility warehouse supervisor.		
c. All tools are etched with departmental identification codes before issuance.		
d. The master and departmental tool inventories are updated whenever new tools are issued to a department.		

B8-8 Tool storage practices at a minimum comply with the following: a. Hazardous tools are stored in a reinforced concrete room with a security key locking system.		
b. Non-hazardous tools are stored in either a secure room with one security key locking system or a secure wire mesh cage with a padlock.		
c. In each location where tools are stored, there are “Shadow Boards” that have a light-colored background with a dark outline of each tool painted on it that facilitates instant identification of a missing tool. The color of the dark outline corresponds to the level of classification of the tool.		
d. If boxes of tools are assigned to areas in the facility, each box is clearly identified as belonging in the area to which it is assigned. Inside each box is an inventory list of all authorized tools.		
B8-9 When a tool is broken or worn out, the facility Tool Control Officer is responsible for documenting the destruction of the tool and revising the master and departmental tool inventories.		
B8-10 All tools brought into the facility on a temporary basis by either a vendor or contractor are inventoried prior to entering the secure perimeter.		
B8-11 Vendors and contractors are under direct supervision by facility personnel while in the secure perimeter.		
B8-12 All tools are re-inventoried before the vendor or contractor is allowed to leave the secure perimeter.		
B8-13 A quarterly audit of all tool control practices is conducted by a supervisory staff member.		
<u>B9.</u> <u>UTILITIES AND MECHANICAL SYSTEMS</u> **B9-1** Staff are able to communicate with each other and the facility control center without interference or interruptions at all times.		
B9-2 Inmates are under direct supervision whenever they are allowed to work on facility telephone and other communications systems. Inmates never have access to two-way communications equipment such as radios.		
B9-3 An emergency lighting system provides illumination for critical areas of the facility in the event of a power failure.		
B9-4 All spaces in which mechanical systems are located are secured from unauthorized access.		
<u>B10. TOXIC/CAUSTICS CONTROL</u> **B10-1** Material Safety Data Sheets are available to identify all toxic, caustic and flammable materials maintained in the facility.		
B10-2 All toxic, caustic and flammable materials are: a. inventoried, and access to them is controlled.		
b. safely stored in appropriate containers and clearly labeled.		
c. utilized under staff supervision.		
d. disposed of in a manner consistent with Material Safety Data Sheets, and the disposal is documented.		

C. PHYSICAL PLANT **C1. LOCATION AND SITE** **C1-1** Inventory forms B1 and B2 are completed (Appendix B).		
C1-2 Inventory forms B1 and B2 are analyzed to identify escape risks posed by: proximity and adjacencies; visibility and observation; continuity; and condition. (See directions in Appendix B) Findings are clearly documented.		
C1-3 The risks identified in C1-2 above are analyzed and, where possible, remedial steps are taken to reduce risks.		
C2. FACILITY DESIGN/LAYOUT and BUILDING CONSTRUCTION **C2-1** Inventory forms B3 and B4 are completed (Appendix B).		
C1-2 Inventory forms B3 and B4 are analyzed to identify escape risks posed by: proximity and adjacencies; visibility and observation; continuity; and condition. (See directions in Appendix B) Findings are clearly documented.		
C1-3 The risks identified in C2-2 above are analyzed and, where possible, remedial steps are taken to reduce risks.		
C3 ENTRANCES AND EXITS IN THE SECURE PERIMETER **C3-1** Whenever there is an opening in the security perimeter, there are at least two interlocked doors or gates that create a secure "sallyport." The gates/doors have an interlock system that allow only one gate or door to be opened at a time. All vehicle gates and sallyport doors are equipped with a manual override system in case of a power outage.		
C3-2 All sallyport doors are controlled from a secure area where inmates and the public have no access.		
C3-3 All persons and vehicles are thoroughly searched prior to allowing entry or exit from the secure perimeter.		
Institutional Visitors **C3-4** All institutional visitors are screened before being allowed entry to the secure perimeter. Visitors entering the secure perimeter are:		
a. the subject of an NCIC inquiry to determine their suitability for visiting.		
b. asked to disclose the purpose of their visit.		
c. asked if they possess any firearms, ammunition, narcotics, and other contraband items.		
d. required to sign in and to affirm in writing that they possess no contraband.		
e. required to present one form of photo identification.		
f. scanned with a metal detector.		
C3-5 A visitor's log is utilized for each visitor to enter name, date, time of visit, purpose of visit and departure time from the secure perimeter. The period of retention for this log is established.		
C3-6 Institutional visitors are under direct supervision by facility personnel while inside the secure perimeter. Exceptions must be approved by the warden or designee.		

C3-7 The facility uses at least two means of identifying visitors before each visitor exits the secure perimeter.		
Vehicles **C3-8** No vehicle is left unattended while in the secure perimeter unless it has been disabled.		
C3-9 All civilian drivers are required to stay inside their vehicle while in the secure perimeter. If it is necessary for them to exit the vehicle, the cab is secured and the keys are retained by escorting personnel.		
C3-10 No civilian vendor with a split delivery load is allowed access to the secure perimeter.		
C3-11 Staff responsible for escorting vehicles inside the secure perimeter do so in such a manner that it allows him/her maximum supervision over the vehicle.		
C3-12 Any vehicle that cannot be thoroughly searched prior to exiting the facility must remain inside the secure facility through at least two official counts. Any vehicle that remains inside the secure perimeter overnight must be rendered inoperable and enhanced security measures are employed.		
C3-13 Enhanced security measures, such as closing inmates access to an area, are made whenever a concrete truck or a truck that has hydraulic lift or crane capabilities is allowed inside the secure perimeter.		
C3-14 Interior and exterior vehicle gates are equipped with crash barriers that are designed to prevent large trucks from compromising the secure perimeter.		
C3-15 All inmates entering or exiting the secure perimeter entrances are positively identified, visually searched, scanned electronically, and a record is maintained of each inmate's name, number, date, time in and out.		
C3-16 There is a duress code that ensures staff in the vehicle gate are not under duress when requesting a vehicle gate to be opened.		
C4. ARMORY **C4-1** The facility maintains an armory with emergency equipment to respond to emergencies and security threats. Armories are located to address internal and external threats.		
C4-2 Armories are constructed to prevent unauthorized entry.		
C4-3 Armories are constructed with a sallyport entry way that is electrically controlled from a remote secure location that has camera monitoring capabilities.		
C4-4 The armory has limited access.		
C4-5 A quarterly inventory all weapons and ammunition is conducted.		
C5. MAIL ROOM **C5-1** The following practices are employed to prevent the introduction of contraband: a. All packages are opened and inspected for contraband prior to entering the secure perimeter.		
b. All mail bags and packages are searched via electronic equipment for the concealment of contraband prior to entering the secure perimeter.		

c. All outgoing letters are screened for possible illegal activity.		
d. All incoming first class mail are physically searched by mail room personnel prior to distribution.		
C5-2 Staff are trained to identify threats that are posed by facility mail. The facility uses resources available from the U.S. Postal Service to enhance staff training and facility safety.		
<u>C6. TRASH COLLECTION/DISPOSAL</u> **C6-1** TRASH TRUCKS. a. If trash trucks are driven by inmates, they are classified as minimum security.		
b. Compacting controls on each truck are operated by facility personnel.		
c. Trash collection and operation of the vehicle are under constant facility personnel supervision.		
d. Trash trucks are rendered inoperable until removed from the secure perimeter.		
e. Trash trucks are left in a secure location through two official counts prior to being allowed to leave the secure perimeter.		
C6-2 TRASH COMPACTOR. a. Keys for the trash compactor are classified as restricted keys and are controlled by staff.		
b, Compacting controls are only operated by facility personnel.		
c. Facility personnel conduct an inmate count of the trash detail prior to, and upon completion of, the trash compacting process.		
d. Facility personnel responsible for the trash compactor detail maintain control over the trash compactor area during the compacting process.		
e. The trash compactor and controls are locked when not in use.		
f. Prior to removing the trash compactor from the secure perimeter, it is relocated to a secure location where enhanced security measures are implemented, and remains in the secure location for a least two official counts prior to being removed from the secure perimeter.		

IV: Operational Checklists

The following pages present specific practices described in Section II according to the specified *frequency.*

<u>EACH SHIFT</u> (or more frequently)

A2-1 g. Supervisory personnel personally receive the count in the control center once during their shift if a count is conducted.

B5-1 Perimeter fences equipped with alarm systems are inspected and tested on a pre-established schedule, to include at a minimum:

a. Staff responsible for monitoring the fence alarm system ensure the system is tested at the control panel at the beginning of each shift.

b. The fence is inspected each shift to ensure no tampering has occurred.

<u>DAILY</u>

A2-1 COUNTS. a. There are at least five official counts conducted during each 24-hour period.

A2-2 CENSUS ACCOUNTABILITY CHECKS. Census accountability checks are conducted in all areas of the facility on a scheduled basis, to determine if all inmates are accounted for and are in their assigned area. The following practices are implemented:

b. An accountability check is conducted each morning of all inmate details and inmates remaining in the housing unit. A second accountability check is conducted after all inmates return to their assigned details after the noon meal. The results of all accountability checks are reported to the control center.

B2-7 Staff check fence alarm and sensor systems at least daily by triggering the alarm in each zone.

B3-2 Walk through metal detectors are will be checked daily by supervisory personnel to ensure they are operational. The results of these checks are recorded.

B5-1 Perimeter fences equipped with alarm systems are inspected and tested on a pre-established schedule, to include at a minimum:

c. Security personnel test the alarm system at least once daily by physically activating each zone.

B6-4 All key rings and keys are counted on a Master Inventory on a daily basis by the Control Center staff.

B8-4 A tool inventory program includes at a minimum:

c. All departments that maintain tools have an identical tool inventory posted with the tools and all tools are accounted for daily.

WEEKLY

A2-2 c. Supervisory personnel conduct impromptu accountability checks in all areas of the facility to ensure assigned inmates are present and/or accounted for. At least one check will be conducted each week, involving at least 10% of the program/work assignments.

A4-8 DISSEMINATION. Intelligence-gathering staff meet weekly with facility administrators to discuss inmates who are believed to be involved in illegal activities, review the list of known escape risks, and discuss strategies.

A5-2 All areas of the facility are searched by respective departmental personnel at least weekly.

A8-1 A comprehensive security inspection program includes at a minimum:
c. Weekly "tapping" of security bars to ensure no tampering has occurred.

B5-7 Supervisory staff inspect all fixed perimeter posts at least weekly to determine if equipment is maintained in good working order and staff are familiar with their responsibilities.

MONTHLY

A2-2 d. Supervisory personnel conduct a total lock-down accountability check of the facility at a minimum of once a month, to ensure all inmates are in their assigned area.

QUARTERLY

A3-3 Emergency Preparedness Drills**:**
b. Emergency preparedness drills are conducted at least quarterly and there is a drill for every plan at least once every 12 months.

B5-4 All weapons assigned to a fixed perimeter post meet the following minimum requirements:
c. Ammunition and weapons are exchanged on at least a quarterly basis.

B5-6 Facility personnel assigned to a fixed perimeter post receive quarterly re-familiarization training on all weapons associated with the post.

B8-4 A tool inventory program includes at a minimum:
e. Tool inventories are conducted by supervisory staff at least quarterly.

B8-13 A quarterly audit of all tool control practices is conducted by a supervisory staff member.

C4-5 A quarterly inventory all weapons and ammunition is conducted.

SEMI-ANNUALLY

A7-12 Escorting staff qualify at a minimum semi-annually with all weapons utilized when escorting inmates outside the secure perimeter.

ANNUALLY

A3-1 Emergency preparedness plans are reviewed annually to ensure the following steps are outlined in response to an inmate escape.

A3-2 The steps necessary to conduct a complete internal search of the facility are described. Plans for internal searches contain, at a minimum:
g. Provisions for review and revision of the plan at least every 12 months.

A3-3 Emergency Preparedness Drills**:**
b. Emergency preparedness drills are conducted at least quarterly and there is a drill for every plan at least once every 12 months.
d. An emergency preparedness drill is conducted with outside law enforcement agencies at least every 12 months to evaluate the memorandum of understanding.

B4-1 A thorough self-analysis is conducted at least annually to identify potential threats for all areas of the facility and to determine potential vulnerabilities from outside threats that could breach the secure perimeter and/or interrupt vital services. This analysis is re-examined whenever there is a substantial change in the physical plant or in the security requirements of the inmate population.

B5-5 Facility personnel assigned to a fixed perimeter post qualify every 12 months with all assigned weapons.

B8-4 A tool inventory program includes at a minimum:
f. Tool inventories are re-issued on an annual basis at a designated time.

UNSPECIFIED FREQUENCY

A1-1 A comprehensive staffing analysis identifies all posts and positions that are required:
a. to maintain security;
b. observe and supervise inmates and inmate-occupied areas, and
c. respond to emergencies.

A5-3 Security personnel periodically conduct departmental searches and document each area searched, the date and the results.

A6-2 There is a record retention schedule for visiting records and related documentation.

B1-3 Video equipment is maintained, inspected, and tested according to manufacturers' specifications.

B1-9 Video surveillance equipment enhances perimeter security and the following requirements are met, at a minimum:
e. Maintenance records are reviewed to determine if surveillance equipment is repaired when malfunctions are reported.

B2-3 Alarm and sensor equipment is maintained, inspected, and tested according to manufacturers' specifications.

B3-5 Metal and other detection equipment is maintained, inspected, and tested according to manufacturers' specifications.

B5-4 All weapons assigned to a fixed perimeter post meet the following minimum requirements:
b. Weapons assigned to a fixed perimeter post are cleaned on a scheduled basis.

B6-3 All locking mechanisms are maintained according to manufacturer's specifications.

C3-5 A visitor's log is utilized for each visitor to enter name, date, time of visit, purpose of visit and departure time from the secure perimeter. *The period of retention for this log is established.*

= = = = = = = = = = = = =

APPENDIX E: Sample PSD's and EASI Results

Sample 1

Foggy, Wednesday, between 5:45 and 6:15 hrs.	Probability of Interruption:	**0.22400**
Inmate collusion - staff hostage -lineman's pliers		

	Alarm		Response Force Time (in Seconds)	
Adversary Sequence	Communi-cation	Pn	Mean	Standard Deviation
Interruption	0.95	1	300	60

Task	Description	P(Detection)	Mean:	Standard Deviation
		Delays (in Seconds):		
1	Collect Trash throughout the facility	0.00	0	0
2	Proceed to checkpoint	0.00	30	15
3	Proceed down the corridor to door number	0.00	30	10
4	Exit door number (?) to dock sidewalk	0.00	30	10
5	Proceed to trash compactor to empty trash	0.00	60	15
6	Attack staff member, hide body under compactor and retrieve set of lineman's pliers left by can man	0.05	60	10
7	Cross dock to parked trailer	0.20	5	2
8	Hide between wheels of parked trailer ensuring perimeter vehicle isn't approaching	0.06	120	15
9	First inmate crawls to internal fence and cuts fence utilizing lineman's pliers.	0.07	36	15
10	First inmate crawls through electronic detection zone	0.20	38	20
11	First inmate cuts inner fence while hiding to ensure perimeter vehicle is not approaching	0.27	73	15
12	First Inmate crawls through restricted area	0.20	2	1
13	First inmate cuts razor wire utilizing lineman's pliers	0.20	20	10
14	First inmate cuts outer fence utilizing lineman's pliers	0.20	36	10
15	Second inmate crawls through internal fence from trailer	0.07	2	1
16	Second inmate crawls through electronic detection zone	0.20	38	10
17	Second inmate crawls through inner fence	0.27	2	1
18	Second inmate crawls through restricted area	0.20	2	1
19	Second inmate crawls through razor wire	0.20	10	5
20	Second inmate crawls through outer fence	0.20	2	1

Sample 2

				Delays (in Seconds):		
Task	Description	P(Detection)	Location	Mean:	Standard Deviation	
1	Arrive at Maintenance, retrieve tools including lineman's pliers, attack/secure staff member	0.2		120	30	
2	Exit door -SV-32	0.1		5	2	
	Run across dock to parked trailer	0.2		11	5	
4	Hide between wheels on trailer	0.03		120	30	
5	Run to internal fence and cut utilizing lineman's pliers	0.07		36	15	
6	Crawl through electronic detection zone (microwave)	0.2		38	20	
7	Cut fence with lineman's pliers ensuring perimeter vehicle does not detect.	0.27		73	30	
8	Cross restricted area	0.2		2	1	
9	Cut razor wire utilizing lineman's pliers	0.2		20	5	**Probability of Interruption**
10	Cut fence with lineman's pliers	0.2		36	10	**0.19123999**

APPENDIX F: DATA COLLECTION FORMS

F1: Entry Control Data Collection Form

Institution: _______________________
Individual Completing Form: _____________________

Location: _______________	Location where the entry control feature is installed. Fill out separate data collection lists for each different type of entry control subsystem.
Type of entry control barriers ☐ Doors ☐ Turnstiles ☐ Gate ☐ None ☐ Other________	Document details of barrier – type, size, thickness, composition, etc.
Type of entry control authorization ☐ Recognition ☐ Picture credential ☐ Picture badge ☐ Coded badge ☐ Code/PIN ☐ Key ☐ Biometric ☐ Other _________	Document details of type of authorization
Control of authorization	Document who, how and when access authorization is granted.
Procedures	Summarize the higher level procedures that will help the team evaluate the effectiveness of the entry control subsystem.
CO Presence	Document the frequency and duration of CO presence near this entry control feature.
Defeat vulnerabilities	Document any observed ways to minimize the intended effect of the entry control feature.
Type of Entry Control: ☐ Metal Detector ☐ X-ray	Document details of search technique

F2. Delay Data Collection Form

Institution: ______________________

Individual Completing Form: ____________________

Location: ______________	Location where the delay feature is installed. Fill out separate data collection lists for each different type of delay.
Type of delay ☐ Solid doors ☐ Bars ☐ Concrete wall ☐ Fence ☐ Razor wire ☐ Vehicle Barriers ☐ Windows ☐ Other_________	Document details of delay – size, thickness, composition, etc.
Detection associated with the delay	Note here and see sensor data collection form for details.
CO Presence	Document the frequency and duration of CO presence near this delay feature.
Defeat vulnerabilities	Document any observed ways to minimize the intended effect of the delay feature.

Appendix G: Performance Data

The following tables present the performance data that is embedded in the “lookup” function of the EASI program. These will allow you find how long certain PPS elements delay an action.

The data contained in the lookup function were developed by Sandia National Laboratories several years ago.

This information should be used as a last resort only, for several reasons:

- It was not initially developed for applications in corrections
- It is not current with the newest technology
- Data that you develop yourself on-site will always be more meaningful.

				Threat Attribute										
Safeguard Class:	Safeguard Type:	Description	Type	No Equipment	Hand Tools	Power Tools	High Explosives	Independent	Land Vehicle	Helicopter	Metal Contraband	Small Arms	Light Antitank Weapons	Radioactive Contraband
Access Control	Bag Port Lock	Combination	DELAY	30000	300	120	30							
Access Control	Bag Port Lock	High security padlock	DELAY	30000	90	60	30							
Access Control	Bag Port Lock	Keyed cylinder	DELAY	30000	20	45	20							
Access Control	Bag Port Lock	Padlock	DELAY	30000	20	40	20							
Access Control	Criticality Alarm	Multiple signals required	PD					0						
Access Control	Criticality Alarm	Multiple simultaneous signals required	PD					0						
Access Control	Criticality Alarm	One signal required	PD					0						
Access Control	Door Penetration Sensor	Conducting tape	PD	80	20	20	90							
Access Control	Door Penetration Sensor	Glass breakage	PD	90	60	60	90							
Access Control	Door Penetration Sensor	Grid mesh	PD	90	60	60	95							
Access Control	Door Penetration Sensor	Multiple sensors	PD	99	90	90	99							
Access Control	Door Penetration Sensor	Vibration	PD	90	40	40	90							
Access Control	Door Position Monitor	Balanced magnetic switch	PD	80	80	80	80		80					
Access Control	Door Position Monitor	Position switch	PD	50	20	20	20		20					
Access Control	Electromagnetic Strike Lock	Casual recognition	DELAY	30000	20	60	20							
Access Control	Electromagnetic Strike Lock	Credential	DELAY	30000	20	60	20							
Access Control	Electromagnetic Strike Lock	Credential and PIN	DELAY	30000	20	60	20							
Access Control	Electromagnetic Strike Lock	Exchange picture badge	DELAY	30000	20	60	20							
Access Control	Electromagnetic Strike Lock	Exchange picture badge and PIN	DELAY	30000	20	60	20							
Access Control	Electromagnetic Strike Lock	Fingerprint and PIN	DELAY	30000	20	60	20							

Access Control	Electromagnetic Strike Lock	Hand geometry and PIN	DELAY	30000	20	60	20							
Access Control	Electromagnetic Strike Lock	Picture badge	DELAY	30000	20	60	20							
Access Control	Electromagnetic Strike Lock	Picture badge and PIN	DELAY	30000	20	60	20							
Access Control	Electromagnetic Strike Lock	Retinal scan and PIN	DELAY	30000	20	60	20							
Access Control	Electromagnetic Strike Lock	Signature dynamics and PIN	DELAY	30000	20	60	20							
Access Control	Electromagnetic Strike Lock	Speech pattern and PIN	DELAY	30000	20	60	20							
Access Control	Evacuation Alarm	Manual activation	PD					0						
Access Control	Evacuation Alarm	Sensor activation	PD					0						
Access Control	Fixed Barrier Penetration Sensor	Conducting tape	PD	80	20	20	90							
Access Control	Fixed Barrier Penetration Sensor	Grid mesh	PD	90	60	60	95							
Access Control	Fixed Barrier Penetration Sensor	Multiple sensors	PD	99	90	90	99							
Access Control	Fixed Barrier Penetration Sensor	Vibration	PD	90	40	40	90							
Access Control	Gate Position Monitor	Balanced magnetic switch	PD	80	80	80	80		80					
Access Control	Gate Position Monitor	Position switch	PD	50	20	20	20		20					
Access Control	Glove Port Lock	Combination	DELAY	30000	300	120	30							
Access Control	Glove Port Lock	High security padlock	DELAY	30000	90	60	30							
Access Control	Glove Port Lock	Keyed cylinder	DELAY	30000	20	45	20							
Access Control	Glove Port Lock	Padlock	DELAY	30000	20	40	20							
Access Control	ID Check	Casual recognition	PD					2						
Access Control	ID Check	Credential	PD					5						
Access Control	ID Check	Credential and PIN	PD					35						
Access Control	ID Check	Exchange picture badge	PD					50						
Access Control	ID Check	Exchange picture badge and PIN	PD					80						
Access Control	ID Check	Fingerprint and PIN	PD					95						
Access Control	ID Check	Hand geometry and PIN	PD					95						
Access Control	ID Check	Picture badge	PD					10						
Access Control	ID Check	Picture badge and PIN	PD					60						
Access Control	ID Check	Retinal scan and PIN	PD					99						

Access Control	ID Check	Signature dynamics and PIN	PD					95						
Access Control	ID Check	Speech pattern and PIN	PD					95						
Access Control	ID Lock Actuator	Casual recognition	PD					2						
Access Control	ID Lock Actuator	Credential	PD					5						
Access Control	ID Lock Actuator	Credential and PIN	PD					35						
Access Control	ID Lock Actuator	Exchange picture badge	PD					50						
Access Control	ID Lock Actuator	Exchange picture badge and PIN	PD					80						
Access Control	ID Lock Actuator	Fingerprint and PIN	PD					95						
Access Control	ID Lock Actuator	Hand geometry and PIN	PD					95						
Access Control	ID Lock Actuator	Picture badge	PD					10						
Access Control	ID Lock Actuator	Picture badge and PIN	PD					60						
Access Control	ID Lock Actuator	Retinal scan and PIN	PD					99						
Access Control	ID Lock Actuator	Signature dynamics and PIN	PD					95						
Access Control	ID Lock Actuator	Speech pattern and PIN	PD					95						
Access Control	Lock	Combination	DELAY	30000	300	120	30							
Access Control	Lock	Electronically coded	DELAY	30000	300	120	30							
Access Control	Lock	High security padlock	DELAY	30000	90	60	30							
Access Control	Lock	Inaccessible	DELAY	30000	30000	30000	30000							
Access Control	Lock	Keyed cylinder	DELAY	30000	20	45	20							
Access Control	Lock	Mechanically coded	DELAY	30000	300	120	30							
Access Control	Lock	Padlock	DELAY	30000	20	40	20							
Access Control	Movable Barrier Penetration Sensor	Conducting tape	PD	80	20	20	90							
Access Control	Movable Barrier Penetration Sensor	Grid mesh	PD	90	60	60	95							
Access Control	Movable Barrier Penetration Sensor	Multiple sensors	PD	99	90	90	99							
Access Control	Movable Barrier Penetration Sensor	Vibration	PD	90	40	40	90							
Access Control	Movable Barrier Position Monitor	Balanced magnetic switch	PD	80	80	80	80		80					
Access Control	Movable Barrier Position Monitor	Position switch	PD	50	20	20	20		20					
Access Control	Personnel Access Authorization Check	Authorization verification each time	PD					60						

		location is accessed												
Access Control	Personnel Access Authorization Check	General observation of authorization	PD					10						
Access Control	Special Drill Control	Observers along evacuation route	PD					0						
Access Control	Special Drill Control	Observers at exit	PD					0						
Access Control	Special Drill Control	Route observers and SNM scan	PD					0						
Access Control	Special Drill Control	SNM scan of personnel	PD					0						
Access Control	Surface Penetration Sensor	Conducting tape	PD	80	20	20	90							
Access Control	Surface Penetration Sensor	Glass breakage	PD	90	60	60	90							
Access Control	Surface Penetration Sensor	Grid mesh	PD	90	60	60	95							
Access Control	Surface Penetration Sensor	Multiple sensors	PD	99	90	90	99							
Access Control	Surface Penetration Sensor	Vibration	PD	90	40	40	90							
Access Control	Tap Lock	Combination	DELAY	30000	300	120	30							
Access Control	Tap Lock	High security padlock	DELAY	30000	90	60	30							
Access Control	Tap Lock	Keyed cylinder	DELAY	30000	20	45	20							
Access Control	Tap Lock	Padlock	DELAY	30000	20	40	20							
Access Control	Two Person Rule	Dedicated observation	PD					50						
Access Control	Two Person Rule	Dedicated observation with alarm	PD					95						
Access Control	Two Person Rule	Presence in area	PD					0						
Access Control	Two Person Rule	Within sight	PD					10						
Access Control	Vehicle Authorization Check	Authorization form check	PD	0					35					
Access Control	Vehicle Authorization Check	Serial number verification	PD	0					45					
Access Control	Vehicle Authorization Check	Visual check of insignia/license plate	PD	0					15					
Access Control	Window Barrier Lock	Combination	DELAY	30000	300	120	30							
Access Control	Window Barrier Lock	High security padlock	DELAY	30000	90	60	30							
Access Control	Window Barrier Lock	Inaccessible	DELAY	30000	30000	30000	30000							
Access Control	Window Barrier Lock	Keyed cylinder	DELAY	30000	20	45	20							
Access Control	Window Barrier Lock	Padlock	DELAY	30000	20	40	20							

Access Control	Window Lock	Combination	DELAY	30000	300	120	30							
Access Control	Window Lock	High security padlock	DELAY	30000	90	60	30							
Access Control	Window Lock	Inaccessible	DELAY	30000	30000	30000	30000							
Access Control	Window Lock	Keyed cylinder	DELAY	30000	20	45	20							
Access Control	Window Lock	Padlock	DELAY	30000	20	40	20							
Access Control	Window Penetration Sensor	Conducting tape	PD	80	20	20	90							
Access Control	Window Penetration Sensor	Glass breakage	PD	90	60	60	90							
Access Control	Window Penetration Sensor	Grid mesh	PD	90	60	60	95							
Access Control	Window Penetration Sensor	Multiple sensors	PD	99	90	90	99							
Access Control	Window Penetration Sensor	Vibration	PD	90	40	40	90							
Access Control	Window Position Monitor	Balanced magnetic switch	PD	80	80	80	80		80					
Access Control	Window Position Monitor	Position switch	PD	50	20	20	20		20					
Access Delay	Bag Port Cover	1/4 inch steel	DELAY	30000	240	180	45							
Access Delay	Bag Port Cover	16 gauge metal	DELAY	30000	120	48	48							
Access Delay	Bag Port Cover	8 gauge metal	DELAY	30000	30	30	30							
Access Delay	Door	1/2 inch steel plate	DELAY	30000	300	30	30		30000					
Access Delay	Door	9 gauge wire mesh	DELAY	30000	30	30	30		30					
Access Delay	Door	Aluminum turnstile	DELAY	30000	72	18	18		30000					
Access Delay	Door	Class V or VI vault	DELAY	30000	480	60	60		30000					
Access Delay	Door	Dispensable barrier	DELAY	0	0	0	0		0					
Access Delay	Door	Half height turnstile	DELAY	1	1	1	1		1					
Access Delay	Door	Hollow core metal	DELAY	30000	12	12	12		12					
Access Delay	Door	Hollow core metal, no lock/hinge protection	DELAY	30000	12	12	12		12					
Access Delay	Door	Igloo	DELAY	30000	300	30	30		30000					
Access Delay	Door	Security glass panel	DELAY	30	30	30	30		30					
Access Delay	Door	Steel turnstile	DELAY	30000	72	18	18		30000					
Access Delay	Door	Tempered glass panel	DELAY	5	5	5	5		5					
Access Delay	Door	Upgraded igloo	DELAY	30000	360	90	90		30000					

Access Delay	Door	Wood	DELAY	30000	12	12	12		12					
Access Delay	Fence	8 foot chainlink	DELAY	10	10	10	10		1					
Access Delay	Fence	8 foot chainlink with outriggers	DELAY	10	10	10	10		1					
Access Delay	Fence	8 foot to 12 foot chainlink with outriggers	DELAY	15	10	10	10		1					
Access Delay	Fence	Over 12 foot chainlink with outriggers	DELAY	20	10	10	10		1					
Access Delay	Fixed Barrier	10 rows of barbed tape	DELAY	30000	60	60	30							
Access Delay	Fixed Barrier	3 mounds of barbed tape	DELAY	30000	30	30	30							
Access Delay	Fixed Barrier	Concertina wire	DELAY	30000	15	10	20							
Access Delay	Fixed Barrier	Triple fence and 2 mounds	DELAY	30000	300	240	60							
Access Delay	Fixed Duct Barrier	16 gauge louvers	DELAY	30000	108	42	42							
Access Delay	Fixed Duct Barrier	Chainlink mesh	DELAY	30000	30	30	30							
Access Delay	Fixed Duct Barrier	Heavy grid	DELAY	30000	720	60	60							
Access Delay	Fixed Duct Barrier	Segmented ducts	DELAY	30000	0	0	0							
Access Delay	Fixed Tunnel Barrier	12 inch filled rebar block	DELAY	30000	900	450	90							
Access Delay	Fixed Tunnel Barrier	16 gauge louvers	DELAY	30000	108	42	42							
Access Delay	Fixed Tunnel Barrier	8 inch filled rebar block	DELAY	30000	450	300	60							
Access Delay	Fixed Tunnel Barrier	8 inch hollow block	DELAY	30000	45	45	30							
Access Delay	Fixed Tunnel Barrier	Chainlink mesh	DELAY	30000	30	30	30							
Access Delay	Fixed Tunnel Barrier	Heavy grid	DELAY	30000	720	60	60							
Access Delay	Fixed Tunnel Barrier	Segmented ducts	DELAY	30000	900	450	300							
Access Delay	Fixed Tunnel Barrier	Wood studs and plywood	DELAY	300	60	90	30							
Access Delay	Fixed Tunnel Barrier	Wood studs and sheetrock	DELAY	60	30	30	30							
Access Delay	Fixed Window Barrier	1/2 inch diameter bars with 6 inch spacing	DELAY	30000	120	30	30							
Access Delay	Fixed Window Barrier	1/2 inch diameter x 1-1/4 inch quarry screen	DELAY	30000	420	180	30							
Access Delay	Fixed Window Barrier	3/16 inch x 2-1/2 inch grating	DELAY	30000	720	60	60							
Access Delay	Fixed Window Barrier	9 gauge expanded mesh	DELAY	30000	30	30	30							

Access Delay	Floor Vault Door	1/2 inch steel plate	DELAY	30000	300	30	30							
Access Delay	Floor Vault Door	Class V or VI vault	DELAY	30000	480	60	60							
Access Delay	Floor Vault Door	Dispensable barrier	DELAY	0	0	0	0							
Access Delay	Gate	8 foot chainlink	DELAY	10	10	10	10		1					
Access Delay	Gate	8 foot chainlink with outriggers	DELAY	10	10	10	10		1					
Access Delay	Gate	8 foot to 12 foot chainlink with outriggers	DELAY	15	10	10	10		1					
Access Delay	Gate	Over 12 foot chainlink with outriggers	DELAY	20	10	10	10		1					
Access Delay	Glove	Reinforced	DELAY	90	20	20	30							
Access Delay	Glove	Standard	DELAY	20	10	10	30							
Access Delay	Glove Port Cover	1/4 inch steel	DELAY	30000	240	180	45							
Access Delay	Glove Port Cover	16 gauge metal	DELAY	30000	120	48	48							
Access Delay	Glove Port Cover	8 gauge metal	DELAY	30000	30	30	30							
Access Delay	Helicopter Load Time	Minimal load time	DELAY	30000						15				
Access Delay	Helicopter Unload Time	Minimal unload time	DELAY	30000						15				
Access Delay	Material Passthrough Door	9 gauge wire mesh	DELAY	30000	30	30	30		30					
Access Delay	Material Passthrough Door	Hollow core metal	DELAY	30000	12	12	12		12					
Access Delay	Material Passthrough Door	Hollow core metal, no lock/hinge protection	DELAY	30000	12	12	12		12					
Access Delay	Material Passthrough Door	Security glass panel	DELAY	30000	30	30	30		30					
Access Delay	Material Passthrough Door	Tempered glass panel	DELAY	300	5	5	5		5					
Access Delay	Material Passthrough Door	Wood	DELAY	30000	12	12	12		12					
Access Delay	Movable Duct Barrier	1/2 inch diameter bars with 6 inch spacing	DELAY	30000	180	60	45							
Access Delay	Movable Duct Barrier	1/4 inch diameter x 1-1/4 inch square mesh	DELAY	30000	720	60	60							
Access Delay	Movable Duct Barrier	16 gauge louvers	DELAY	30000	108	42	42							
Access Delay	Movable Duct Barrier	3/16 inch x 2-1/4 inch grating	DELAY	30000	720	60	60							
Access Delay	Movable Duct Barrier	3/8 inch diameter x 1-1/4 inch square mesh	DELAY	30000	1200	300	60							

Access Delay	Movable Duct Barrier	9 gauge expanded mesh	DELAY	30000	30	30	30							
Access Delay	Movable Tunnel Barrier	1/2 inch diameter bars with 6 inch spacing	DELAY	30000	150	60	45							
Access Delay	Movable Tunnel Barrier	1/2 inch steel plate	DELAY	30000	300	30	30							
Access Delay	Movable Tunnel Barrier	1/4 inch diameter x 1-1/4 inch square mesh	DELAY	30000	720	60	60							
Access Delay	Movable Tunnel Barrier	16 gauge louvers	DELAY	30000	108	42	42							
Access Delay	Movable Tunnel Barrier	3/16 inch x 2-1/4 inch grating	DELAY	30000	720	60	60							
Access Delay	Movable Tunnel Barrier	3/8 inch diameter x 1-1/4 inch square mesh	DELAY	30000	1200	300	60							
Access Delay	Movable Tunnel Barrier	9 gauge expanded mesh	DELAY	30000	30	30	30							
Access Delay	Movable Tunnel Barrier	Dispensable barrier	DELAY	0	0	0	0							
Access Delay	Movable Tunnel Barrier	Hollow core metal	DELAY	30000	12	12	12							
Access Delay	Movable Tunnel Barrier	Hollow core metal, no lock/hinge protection	DELAY	30000	12	12	12							
Access Delay	Movable Tunnel Barrier	Security glass panel	DELAY	30000	30	30	30							
Access Delay	Movable Window Barrier	1/2 inch diameter bars with 6 inch spacing	DELAY	30000	120	30	30							
Access Delay	Movable Window Barrier	1/2 inch diameter x 1-1/4 inch quarry screen	DELAY	30000	420	180	30							
Access Delay	Movable Window Barrier	3/16 inch x 2-1/2 inch grating	DELAY	30000	720	60	60							
Access Delay	Movable Window Barrier	9 gauge expanded mesh	DELAY	30000	30	30	30							
Access Delay	Openable Window	Acrylic plastic	DELAY	180	30	30	20							
Access Delay	Openable Window	Laminated glass	DELAY	30000	90	45	20							
Access Delay	Openable Window	Polycarbonate plastic	DELAY	30000	90	45	30							
Access Delay	Openable Window	Security glass	DELAY	30000	180	90	30							
Access Delay	Openable Window	Tempered glass	DELAY	300	30	20	20							
Access Delay	Removable Barrier	King Tut block	DELAY	30000	30000	1200	180		180					
Access Delay	Surface Stage 1 Delay	1/2 inch wood roof	DELAY	30000	180	120	60		30000					
Access Delay	Surface Stage 1 Delay	10 foot earth cover	DELAY	30000	900	180	60		30000					
Access Delay	Surface Stage 1 Delay	10 foot soil cement earth cover	DELAY	30000	900	180	60		30000					

Access Delay	Surface Stage 1 Delay	12 inch filled rebar block	DELAY	30000	800	500	80		30000					
Access Delay	Surface Stage 1 Delay	12 inch reinforced concrete	DELAY	30000	30000	600	120		30000					
Access Delay	Surface Stage 1 Delay	16 gauge metal	DELAY	30000	108	42	42		5					
Access Delay	Surface Stage 1 Delay	2 inch precast concrete tee	DELAY	30000	60	60	120		30000					
Access Delay	Surface Stage 1 Delay	20 gauge metal built up roof	DELAY	30000	180	130	60		30000					
Access Delay	Surface Stage 1 Delay	20 gauge metal with insulation	DELAY	30000	120	48	48		30000					
Access Delay	Surface Stage 1 Delay	24 inch reinforced concrete	DELAY	30000	30000	900	180		30000					
Access Delay	Surface Stage 1 Delay	3 foot earth cover	DELAY	30000	300	240	120		120					
Access Delay	Surface Stage 1 Delay	3 foot soil cement earth cover	DELAY	30000	900	180	60		30000					
Access Delay	Surface Stage 1 Delay	4 inch reinforced concrete	DELAY	30000	280	280	84		30000					
Access Delay	Surface Stage 1 Delay	5-1/2 inch concrete roof	DELAY	30000	240	210	90		30000					
Access Delay	Surface Stage 1 Delay	8 inch concrete roof	DELAY	30000	30000	240	180		30000					
Access Delay	Surface Stage 1 Delay	8 inch filled block	DELAY	30000	150	100	60		5					
Access Delay	Surface Stage 1 Delay	8 inch filled rebar block	DELAY	30000	450	300	90		30000					
Access Delay	Surface Stage 1 Delay	8 inch hollow block	DELAY	30000	50	50	30		5					
Access Delay	Surface Stage 1 Delay	8 inch reinforced concrete	DELAY	30000	30000	840	120		30000					
Access Delay	Surface Stage 1 Delay	Chainlink mesh	DELAY	30000	10	10	10		5					
Access Delay	Surface Stage 1 Delay	Clay block	DELAY	30000	150	30	30		5					
Access Delay	Surface Stage 1 Delay	Concrete built up roof with T beam	DELAY	30000	210	180	60		30000					
Access Delay	Surface Stage 1 Delay	Dispensable barrier	DELAY	0	0	0	0		0					
Access Delay	Surface Stage 1 Delay	Wood studs and plywood	DELAY	120	60	90	30		5					
Access Delay	Surface Stage 1 Delay	Wood studs and sheetrock	DELAY	60	30	30	30		5					
Access Delay	Surface Stage 2 Delay	1/2 inch wood roof	DELAY	30000	0	0	0		30000					
Access Delay	Surface Stage 2 Delay	10 foot earth cover	DELAY	30000	1800	450	90		30000					
Access Delay	Surface Stage 2 Delay	10 foot soil cement earth cover	DELAY	30000	1800	450	90		30000					
Access Delay	Surface Stage 2 Delay	12 inch filled rebar block	DELAY	30000	0	0	0		30000					
Access Delay	Surface Stage 2 Delay	12 inch reinforced concrete	DELAY	30000	30000	1200	54		30000					
Access Delay	Surface Stage 2 Delay	16 gauge metal	DELAY	30000	0	0	0		0					

Access Delay	Surface Stage 2 Delay	2 inch precast concrete tee	DELAY	30000	0	0	0		30000					
Access Delay	Surface Stage 2 Delay	20 gauge metal built up roof	DELAY	30000	0	0	0		30000					
Access Delay	Surface Stage 2 Delay	20 gauge metal with insulation	DELAY	30000	0	0	0		30000					
Access Delay	Surface Stage 2 Delay	24 inch reinforced concrete	DELAY	30000	30000	1800	300		30000					
Access Delay	Surface Stage 2 Delay	3 foot earth cover	DELAY	30000	0	0	0		30000					
Access Delay	Surface Stage 2 Delay	3 foot soil cement earth cover	DELAY	30000	1800	450	90		30000					
Access Delay	Surface Stage 2 Delay	4 inch reinforced concrete	DELAY	30000	0	0	0		30000					
Access Delay	Surface Stage 2 Delay	5-1/2 inch concrete roof	DELAY	30000	200	200	0		30000					
Access Delay	Surface Stage 2 Delay	8 inch concrete roof	DELAY	30000	30000	400	0		30000					
Access Delay	Surface Stage 2 Delay	8 inch filled block	DELAY	30000	0	0	0		0					
Access Delay	Surface Stage 2 Delay	8 inch filled rebar block	DELAY	30000	0	0	0		30000					
Access Delay	Surface Stage 2 Delay	8 inch hollow block	DELAY	30000	0	0	0		0					
Access Delay	Surface Stage 2 Delay	8 inch reinforced concrete	DELAY	30000	0	0	0		30000					
Access Delay	Surface Stage 2 Delay	Chainlink mesh	DELAY	0	0	0	0		0					
Access Delay	Surface Stage 2 Delay	Clay block	DELAY	30000	0	0	0		0					
Access Delay	Surface Stage 2 Delay	Concrete built up roof with T beam	DELAY	30000	0	0	0		30000					
Access Delay	Surface Stage 2 Delay	Dispensable barrier	DELAY	0	0	0	0		0					
Access Delay	Surface Stage 2 Delay	Wood studs and plywood	DELAY	0	0	0	0		0					
Access Delay	Surface Stage 2 Delay	Wood studs and sheetrock	DELAY	0	0	0	0		0					
Access Delay	Target Enclosure Door	9 gauge wire mesh	DELAY	30000	30	30	30		30					
Access Delay	Target Enclosure Door	Hollow core metal	DELAY	30000	12	12	12		12					
Access Delay	Target Enclosure Door	Hollow core metal, no lock/hinge protection	DELAY	30000	12	12	12		12					
Access Delay	Target Enclosure Door	Security glass panel	DELAY	30000	30	30	30		30					
Access Delay	Target Enclosure Door	Tempered glass panel	DELAY	300	5	5	5		5					
Access Delay	Target Enclosure Door	Wood	DELAY	30000	12	12	12		12					
Access Delay	Target Enclosure Surface	1/2 inch diameter bars with 6 inch spacing	DELAY	30000	180	60	45							
Access Delay	Target Enclosure Surface	1/4 inch diameter x 1-1/4 inch square mesh	DELAY	30000	720	60	60							

Access Delay	Target Enclosure Surface	16 gauge metal	DELAY	30000	108	42	42							
Access Delay	Target Enclosure Surface	3/16 inch x 2-1/4 inch grating	DELAY	30000	720	60	60							
Access Delay	Target Enclosure Surface	3/8 inch diameter x 1-1/4 inch square mesh	DELAY	30000	1200	300	60							
Access Delay	Target Enclosure Surface	9 gauge expanded mesh	DELAY	30000	30	30	30							
Access Delay	Target Enclosure Surface	Acrylic plastic	DELAY	120	30	30	20							
Access Delay	Target Enclosure Surface	Laminated glass	DELAY	30000	150	60	30							
Access Delay	Target Enclosure Surface	Polycarbonate plastic	DELAY	30000	150	60	30							
Access Delay	Target Enclosure Surface	Security glass	DELAY	30000	120	60	30							
Access Delay	Target Enclosure Surface	Tempered glass	DELAY	300	5	5	5							
Access Delay	Target Enclosure Surface	Wood studs and plywood	DELAY	300	60	90	30							
Access Delay	Target Enclosure Surface	Wood studs and sheetrock	DELAY	60	30	30	30							
Access Delay	Target Task Time	Dispensable delay	DELAY	0	0	0	0							
Access Delay	Target Task Time	Minimal task time	DELAY	15	15	15	15							
Access Delay	Tie Downs	Metal strap secured with bolt	DELAY	30000	20	10	20							
Access Delay	Tie Downs	Metal strap secured with lock	DELAY	30000	20	10	20							
Access Delay	Tie Downs	Nylon web secured with bolt	DELAY	30000	20	10	20							
Access Delay	Tie Downs	Nylon web secured with lock	DELAY	30000	20	10	20							
Access Delay	Tie Downs	Wire secured with bolt	DELAY	30000	30	15	20							
Access Delay	Tie Downs	Wire secured with lock	DELAY	30000	20	10	20							
Access Delay	Unopenable Window	Acrylic plastic	DELAY	180	30	30	20							
Access Delay	Unopenable Window	Laminated glass	DELAY	30000	90	45	20							
Access Delay	Unopenable Window	Polycarbonate plastic	DELAY	30000	90	45	30							
Access Delay	Unopenable Window	Security glass	DELAY	30000	180	90	30							
Access Delay	Unopenable Window	Tempered glass	DELAY	300	30	20	20							
Access Delay	Vehicle Barrier	Aircraft cable	DELAY	0	120	45	45		30					
Access Delay	Vehicle Barrier	Bollard	DELAY	0	720	180	30		5					
Access Delay	Vehicle Barrier	Concrete blocks	DELAY	0	300	300	30		5					
Access Delay	Vehicle Barrier	Concrete median	DELAY	0	200	120	60		30					

Access Delay	Vehicle Barrier	Concrete median and ditch	DELAY	0	960	360	360		360					
Access Delay	Vehicle Barrier	Crash I beam	DELAY	0	1440	240	60		30					
Access Delay	Vehicle Barrier	Guard rails	DELAY	0	720	180	90		5					
Access Delay	Vehicle Barrier	Hydraulic wedge	DELAY	0	300	240	60		30					
Access Delay	Vehicle Barrier	Steel posts	DELAY	0	720	240	30		30					
Access Delay	Vehicle Barrier	Train barrier	DELAY	0	1440	240	60		30					
Access Delay	Vehicle/Personnel Door	1/2 inch steel plate	DELAY	30000	300	30	30		30000					
Access Delay	Vehicle/Personnel Door	9 gauge wire mesh	DELAY	30000	30	30	30		30					
Access Delay	Vehicle/Personnel Door	Dispensable barrier	DELAY	0	0	0	0		0					
Access Delay	Vehicle/Personnel Door	Hollow core metal	DELAY	30000	12	12	12		12					
Access Delay	Vehicle/Personnel Door	Hollow core metal, no lock/hinge protection	DELAY	30000	12	12	12		12					
Access Delay	Vehicle/Personnel Door	Security glass panel	DELAY	30000	30	30	30		30					
Access Delay	Vehicle/Personnel Door	Tempered glass panel	DELAY	300	5	5	5		5					
Access Delay	Vehicle/Personnel Door	Vehicle liftup	DELAY	30000	108	42	42		60					
Access Delay	Vehicle/Personnel Door	Vehicle rollup	DELAY	30000	108	42	42		60					
Access Delay	Vehicle/Personnel Door	Wood	DELAY	30000	12	12	12		12					
Contraband Detection	Explosives Detector	Animal olfaction	PD	0			10							
Contraband Detection	Explosives Detector	Handheld vapor collection	PD	0			45							
Contraband Detection	Explosives Detector	Thermal neutron	PD	0			25							
Contraband Detection	Explosives Detector	Vapor collection	PD	0			35							
Contraband Detection	Handheld Metal Detector	Ferrous and solid lead materials	PD	0	85	75					25	50		
Contraband Detection	Handheld Metal Detector	Ferrous materials and all forms of lead	PD	0	85	75					25	50		
Contraband Detection	Handheld Metal Detector	Ferrous materials only	PD	0	85	75					25	50		
Contraband Detection	Item Search	Cursory	PD	0	10	10	10							10
Contraband Detection	Item Search	Rigorous	PD	0	75	75	45							65
Contraband Detection	Personnel Search	Patdown	PD	0	90	90	30							90
Contraband Detection	Personnel Search	Strip inspection	PD	0	90	90	90							90

Contraband Detection	Portal Metal Detector	Ferrous and solid lead materials	PD	0	90	90					80	60		
Contraband Detection	Portal Metal Detector	Ferrous materials and all forms of lead	PD	0	90	90					80	60		
Contraband Detection	Portal Metal Detector	Ferrous materials only	PD	0	90	90					80	60		
Contraband Detection	Vehicle Search	Cursory	PD	0	10	10	10							10
Contraband Detection	Vehicle Search	Rigorous including cargo	PD	0	50	50	25							40
Contraband Detection	X-Ray Inspection	Standard	PD	0	90	90						60		90
Intrusion Detection	Air Contamination Monitor	Alpha particle	PD					0						
Intrusion Detection	Air Pressure Monitor	Remote readout	PD					0						
Intrusion Detection	Air Pressure Monitor	Visual check	PD					0						
Intrusion Detection	Bag Port Penetration Sensor	Conducting tape	PD	80	20	20	90							
Intrusion Detection	Bag Port Penetration Sensor	Grid mesh	PD	90	60	60	95							
Intrusion Detection	Bag Port Penetration Sensor	Multiple sensors	PD	99	90	90	99							
Intrusion Detection	Bag Port Penetration Sensor	Vibration	PD	90	40	40	90							
Intrusion Detection	Bag Port Position Monitor	Balanced magnetic switch	PD	80	80	80	80		80					
Intrusion Detection	Bag Port Position Monitor	Position switch	PD	50	20	20	20		20					
Intrusion Detection	Container Tamper Monitor	Remote readout	PD					0						
Intrusion Detection	Container Tamper Monitor	Visual check	PD					0						
Intrusion Detection	Exterior Intrusion Sensors	Electric field	PD	50	30	30	50		90					
Intrusion Detection	Exterior Intrusion Sensors	Infrared	PD	80	40	40	50		80					
Intrusion Detection	Exterior Intrusion Sensors	Microwave	PD	80	70	70	70		90					
Intrusion Detection	Exterior Intrusion Sensors	Multiple complementary sensors	PD	99	95	95	99		99					
Intrusion Detection	Exterior Intrusion Sensors	Multiple noncomplementary sensors	PD	90	80	80	80		99					
Intrusion Detection	Exterior Intrusion Sensors	Seismic buried cable	PD	50	50	50	50		90					
Intrusion Detection	Exterior Intrusion Sensors	Video motion	PD	80	60	60	70		90					
Intrusion Detection	Fence Sensor	Electric field	PD	50	40	40	75		90					
Intrusion Detection	Fence Sensor	Multiple sensors	PD	75	50	50	80		90					
Intrusion Detection	Fence Sensor	Strain	PD	10	10	10	10		90					

Intrusion Detection	Fence Sensor	Taut wire	PD	50	25	25	75		85					
Intrusion Detection	Fence Sensor	Vibration	PD	50	10	10	75		85					
Intrusion Detection	Flow Rate Monitor	Remote readout	PD					0						
Intrusion Detection	Flow Rate Monitor	Visual check	PD					0						
Intrusion Detection	Fluid Level Monitor	Remote readout	PD					0						
Intrusion Detection	Fluid Level Monitor	Visual check	PD					0						
Intrusion Detection	Fluid Pressure Monitor	Remote readout	PD					0						
Intrusion Detection	Fluid Pressure Monitor	Visual check	PD					0						
Intrusion Detection	Gate Sensor	Electric field	PD	50	40	40	75		90					
Intrusion Detection	Gate Sensor	Multiple sensors	PD	75	50	50	80		90					
Intrusion Detection	Gate Sensor	Strain	PD	10	10	10	10		90					
Intrusion Detection	Gate Sensor	Taut wire	PD	50	25	25	75		85					
Intrusion Detection	Gate Sensor	Vibration	PD	50	10	10	75		85					
Intrusion Detection	General Observation	Personnel always in vicinity	PD					2						
Intrusion Detection	General Observation	Personnel generally in vicinity	PD					1						
Intrusion Detection	Glove Penetration Sensor	Conducting tape	PD	80	20	20	90							
Intrusion Detection	Glove Penetration Sensor	Grid mesh	PD	90	60	60	95							
Intrusion Detection	Glove Penetration Sensor	Multiple sensors	PD	99	90	90	99							
Intrusion Detection	Glove Penetration Sensor	Vibration	PD	90	40	40	90							
Intrusion Detection	Glove Port Penetration Sensor	Conducting tape	PD	80	20	20	90							
Intrusion Detection	Glove Port Penetration Sensor	Grid mesh	PD	90	60	60	95							
Intrusion Detection	Glove Port Penetration Sensor	Multiple sensors	PD	99	90	90	99							
Intrusion Detection	Glove Port Penetration Sensor	Vibration	PD	90	40	40	90							
Intrusion Detection	Glove Port Position Monitor	Balanced magnetic switch	PD	80	80	80	80		80					
Intrusion Detection	Glove Port Position Monitor	Position switch	PD	50	20	20	20		20					
Intrusion Detection	Helicopter Detector	Radar	PD	0						10				
Intrusion Detection	Helicopter Detector	Sonic	PD	0						10				
Intrusion Detection	Interior Intrusion Sensors	Capacitance	PD	50	50	50	50							

Intrusion Detection	Interior Intrusion Sensors	Infrared	PD	50	50	50	50							
Intrusion Detection	Interior Intrusion Sensors	Microwave	PD	50	50	50	50							
Intrusion Detection	Interior Intrusion Sensors	Multiple complementary sensors	PD	90	90	90	90							
Intrusion Detection	Interior Intrusion Sensors	Multiple noncomplementary sensors	PD	75	75	75	75							
Intrusion Detection	Interior Intrusion Sensors	Sonic	PD	50	50	50	50							
Intrusion Detection	Interior Intrusion Sensors	Ultrasonic	PD	50	50	50	50							
Intrusion Detection	Interior Intrusion Sensors	Video motion	PD	50	50	50	50							
Intrusion Detection	Item Counter	Beam count	PD					0						
Intrusion Detection	Item Counter	Mechanical count	PD					0						
Intrusion Detection	Item Counter	Visual count	PD					0						
Intrusion Detection	Item Presence Sensor	Balanced magnetic switch	PD	90	86	85	90							
Intrusion Detection	Item Presence Sensor	Capacitance	PD	70	60	60	80							
Intrusion Detection	Item Presence Sensor	Pressure pad	PD	40	40	40	95							
Intrusion Detection	Tap Position Monitor	Balanced magnetic switch	PD	80	80	80	80		80					
Intrusion Detection	Tap Position Monitor	Position switch	PD	50	20	20	20		20					
Intrusion Detection	Weight Pad	Capacitance	PD	60	40	40	90							
Intrusion Detection	Weight Pad	Weight/Pressure	PD	40	40	40	40							
Security Inspectors	SI at Post Delay	Duress, LAW protected	DELAY	30000								125	125	
Security Inspectors	SI at Post Delay	Duress, small arms protected	DELAY	30000								30	0	
Security Inspectors	SI at Post Delay	Duress, small arms protected: LAW prot on alert	DELAY	30000								125	125	
Security Inspectors	SI at Post Delay	Duress, unprotected	DELAY	30000								0	0	
Security Inspectors	SI at Post Delay	Duress, unprotected: LAW prot on alert	DELAY	30000								125	125	
Security Inspectors	SI at Post Delay	Duress, unprotected: small arms prot on alert	DELAY	30000								30	0	
Security Inspectors	SI at Post Delay	No duress, LAW protected	DELAY	30000								125	125	
Security Inspectors	SI at Post Delay	No duress, small arms protected	DELAY	30000								30	0	
Security Inspectors	SI at Post Delay	No duress, small arms protected:	DELAY	30000								125	125	

		LAW prot on alert												
Security Inspectors	SI at Post Delay	No duress, unprotected	DELAY	30000								0	0	
Security Inspectors	SI at Post Delay	No duress, unprotected: LAW prot on alert	DELAY	30000								125	125	
Security Inspectors	SI at Post Delay	No duress, unprotected: small arms prot on alert	DELAY	30000								30	0	
Security Inspectors	SI at Post Observation	Duress, LAW protected	PD	80								80	80	
Security Inspectors	SI at Post Observation	Duress, small arms protected	PD	80								80	45	
Security Inspectors	SI at Post Observation	Duress, small arms protected: LAW prot on alert	PD	80								80	45	
Security Inspectors	SI at Post Observation	Duress, unprotected	PD	80								45	45	
Security Inspectors	SI at Post Observation	Duress, unprotected: LAW prot on alert	PD	80								45	45	
Security Inspectors	SI at Post Observation	Duress, unprotected: small arms prot on alert	PD	80								45	45	
Security Inspectors	SI at Post Observation	No duress, LAW protected	PD	80								80	45	
Security Inspectors	SI at Post Observation	No duress, small arms protected	PD	80								45	45	
Security Inspectors	SI at Post Observation	No duress, small arms protected: LAW prot on alert	PD	80								45	45	
Security Inspectors	SI at Post Observation	No duress, unprotected	PD	80								0	0	
Security Inspectors	SI at Post Observation	No duress, unprotected: LAW prot on alert	PD	80								0	0	
Security Inspectors	SI at Post Observation	No duress, unprotected: small arms prot on alert	PD	80								0	0	
Security Inspectors	SI in Tower Delay	LAW resistant tower	DELAY	125								125	60	
Security Inspectors	SI in Tower Delay	Small arms resistant	DELAY	60								30	0	
Security Inspectors	SI in Tower Observation	LAW resistant tower	PD	5								5	2	
Security Inspectors	SI in Tower Observation	Small arms resistant	PD	5								5	2	
Security Inspectors	SI on Patrol	Random	PD					2						
Security Inspectors	SI on Patrol	Scheduled	PD					1						
SNM Detection	Drive Thru SNM Monitor	Plastic scintillator	PD	0										50
SNM Detection	Drive Thru SNM Monitor	Sodium iodide scintillator	PD	0										50

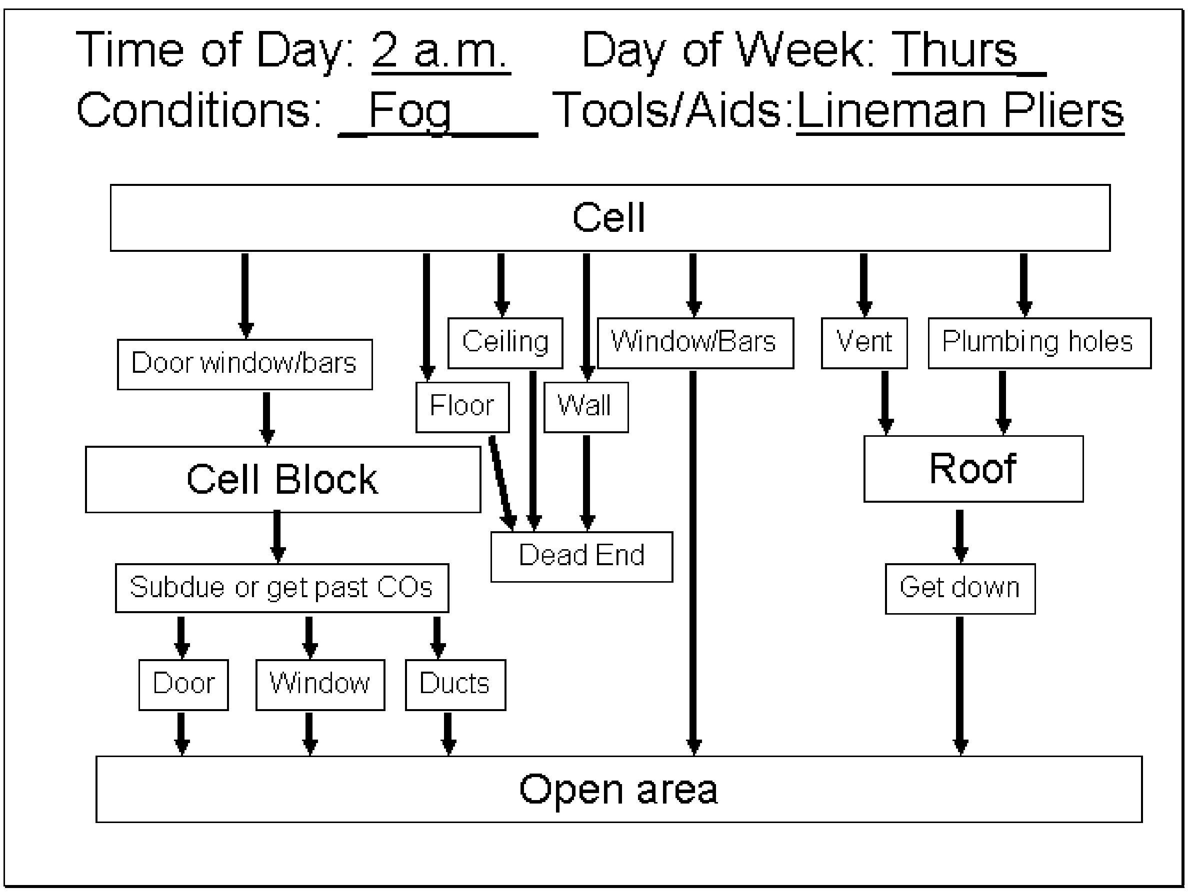
SNM Detection	Handheld SNM Monitor	Plastic scintillator	PD	0										75
SNM Detection	Handheld SNM Monitor	Sodium iodide scintillator	PD	0										75
SNM Detection	Portal SNM Monitor	Plastic scintillator	PD	0										85
SNM Detection	Portal SNM Monitor	Sodium iodide scintillator	PD	0										85

Appendix H: PSD Checklist

The following chart may be helpful as a template for making your own Path Sequence Diagrams (PSDs).

Be sure to note:

- Time of day
- Day of week
- Conditions (weather, staffing, other)
- Tools and aids considered



[

Appendix I: Acronyms and Selected EASI Formulas

The CVA process uses many technical terms and it is often convenient to use acronyms rather than spelling out every phrase. The following list contains the acronyms you are likely to encounter when conducting a CVA.

ACRONYMS

ABSPO	activation by sally port officer
B	beginning (as used in timing of detection)
CI	correctional industries
CO	correctional officer
CRO	control room officer
E	end (as used in timing of detection)
EASI	Estimate of Adversary Sequence Interruption
H	high
L	low
M	medium
M	middle (as used in timing of detection)
MW	microwave
PD	probability of detection
PI	probability of interruption
PN	probability of neutralization
PPS	physical protection system
PSD	path sequence diagram
PTZ	pan/tilt/zoom
RF	response force
RFT	response force time
RHU	restricted housing unit
SCI	State Correctional Institution
SNL	Sandia National Laboratories
TL VCR	time-lapse videocassette recorder
VA	vulnerability analysis
OBG	observation by guard
Snw	sensor not working
MWnw	microwave not working
OBT	observation by tower
VO	video observation
OBS	observation by staff
OBOSP	observation by outside security patrol
EO	expert opinion

The EASI program applies a complex series of calculations to the information and data that is entered. Formulas that might be used to calculate the "probability of neutralization" (P_N) are shown below.

Method for Estimating P_N

For Escapes:

- P_N = .8 - .9 where the one armed CO is interposed in the path before one escapee
- Increase if more COs and decreases if more escapees
- P_N = .3 - .5 where an unarmed CO is interposed in the path

For Contraband

- P_N = 1.0 once the contraband has been discovered

For outsider and active-violent insider scenario risk calculation:

Assume: $P_N = 1$, $P_A = 1$, $C = 1$ where Risk $(R) = 1\text{-}P_D$

$$\text{Risk } (R) = P_A * [1 - (P_I * P_N)] * C$$

Non-Violent Insider (e.g. contraband) risk calculation:

$$\text{Risk } (R) = P_A * [1\text{-}P_D] * C$$

APPENDIX J: Excerpts from *Core Jail Standards*[1]

The following pages present selected standards and practices that have a direct or indirect relationship with jail safety, security and vulnerability.

1. SAFETY

GOAL: Provide a safe environment for the community, staff, and inmates.

PERFORMANCE STANDARD
1A. The community, staff, contractors, volunteers, and inmates are protected from injury and illness caused by the physical environment.

Expected Practices

The facility complies with all applicable laws and regulations of the governing jurisdiction. 4-ALDF-1A-01 (MANDATORY)

Disposal of liquid, solid, and hazardous material complies with applicable government regulations. 4-ALDF-1A-02 (MANDATORY)

The facility is clean and in good repair. 4-ALDF-1A-04

Lighting throughout the facility is sufficient for the tasks performed. 4-ALDF-1A-14

Non-smoking inmates are not exposed to second-hand smoke. 4-ALDF-1A-21

PERFORMANCE STANDARD

1C. The number and severity of emergencies are minimized. When emergencies occur, the response minimizes the severity.
Definition: An emergency is any event that results in the suspension or disruption of normal facility operations.

Expected Practices

There is a plan that guides the facility response to emergencies. All facility personnel are trained annually in the implementation of the emergency plan. 4-ALDF-1C-01 (MANDATORY)

[1]American Correctional Association, Alexandria, VA. 2009.

An evacuation plan is used in the event of fire or major emergency. The plan is approved by an independent outside inspector trained in the application of national fire safety codes and is reviewed annually, updated if necessary, and reissued to the local fire jurisdiction. 4-ALDF-1C-02 (MANDATORY)

There is a means for the immediate release of inmates from locked areas in case of emergency and provisions for a backup system.
4-ALDF-1C-03 (MANDATORY)

The facility has exits that are properly positioned, are clear from obstruction, and are distinctly and permanently marked to ensure the timely evacuation of inmates and staff in the event of fire or other emergency. All housing areas and places of assembly for 50 or more persons have two exits.
4-ALDF-1C-04 (MANDATORY)

The facility conforms to applicable federal, state, and/or local fire safety codes.
4-ALDF-1C-07 (MANDATORY)

The facility's fire prevention regulations and practices ensure the safety of staff, inmates, and visitors. 4-ALDF-1C-08 (MANDATORY)

There is a comprehensive and thorough monthly inspection of the facility by a qualified fire and safety officer for compliance with safety and fire prevention standards. 4-ALDF-1C-09 (MANDATORY)

Facility furnishings meet fire safety performance requirements.
4-ALDF-1C-10 (MANDATORY)

Flammable, toxic, and caustic materials are controlled and used safely.
4-ALDF-1C-11 (MANDATORY)

Essential lighting and life-sustaining functions are maintained inside the facility and with the community in an emergency.
4-ALDF-1C-12 (MANDATORY)

2. SECURITY

GOAL: Protect the community, staff, contractors, volunteers, and inmates from harm.

PERFORMANCE STANDARD

2A. The community, staff, contractors, volunteers, and inmates are protected from harm. Events that pose risk of harm are prevented. The number and severity of events are minimized.

Expected Practices

The facility's security, life safety, and communications systems are monitored continuously from a secure location. 4-ALDF-2A-01

The use of padlocks in place of security locks on cell or inmate housing unit doors is prohibited.

A shift commander must be physically onsite 24 hours a day.

Correctional officer posts are located adjacent to inmate living areas to permit officers to see or hear and respond promptly to emergency situations. 4-ALDF-2A-03

There are written orders for every correctional officer post. 4-ALDF-2A-04

The facility administrator or designee visits the facility's living and activity areas at least weekly. 4-ALDF-2A-06

The facility perimeter ensures inmates are secured and that access by the general public is denied without proper authorization. 4-ALDF-2A-07

When a female is housed in a facility, at least one female staff member is on duty at all times. 4-ALDF-2A-08

No inmate or group of inmates is given control, or allowed to exert authority, over other inmates. 4-ALDF-2A-09

All inmate movement from one area to another is controlled by staff. 4-ALDF-2A-10

Correctional staff maintains a permanent log and prepare shift reports that record routine information, emergency situations, and unusual incidents. 4-ALDF-2A-11

Sufficient staff are provided at all times to perform functions relating to the security, custody, and supervision of inmates and as needed to operate the facility in conformance with the standards. 4-ALDF-2A-14

There is an inmate population management process that includes records on the admission, processing, and release of inmates. 4-ALDF-2A-16

The facility has a system for physically counting inmates. At least one formal count is conducted for each shift, with no less than three counts daily. 4-ALDF-2A-17

Physical plant designs facilitate continuous personal contact and interaction between staff and inmates in housing units. All living areas are constructed to facilitate continuous staff observation, excluding electronic surveillance, of cell or detention room fronts and areas such as dayrooms and recreation spaces. (Renovation, addition, new construction only). 4-ALDF-2A-18

Prior to accepting custody of an inmate, staff determines that the inmate is legally committed to the facility, and that the inmate is not in need of immediate medical attention that is not available at the facility. 4-ALDF-2A-19

The inmate and his/her personal property are immediately searched upon arrival at the facility. 4-ALDF-2A-20

Admission processes for a newly-admitted inmate include, but are not limited to:

- basic personal data
- criminal history check
- photographing and fingerprinting as required
- medical, dental, and mental health screening
- suicide screening

4-ALDF-2A-21

There is an itemized inventory of all personal property of newly-admitted inmates and secure storage of inmate property, including money and other valuables. The inmate is given a receipt for all property held until release. 4-ALDF-2A-23.

Prior to being placed in the general population, each inmate is provided with an orientation and continuing access to the facility rules and regulations, including access to medical care. The written materials are translated into those languages spoken by significant number of inmates. 4-ALDF-2A-27

Information is provided to inmates about sexual abuse/assault including:

- prevention/intervention
- self-protection
- reporting sexual abuse/assault
- treatment and counseling

The information is communicated orally and in writing, in a language clearly understood by the inmate, upon arrival at the facility. 4-ALDF-2A-29

Sexual conduct between staff and detainees, volunteers or contract personnel and detainees, regardless of consensual status, is prohibited and subject to administrative, disciplinary and criminal sanctions. 4-ALDF-2A-29-1

An objective classification system is used to separate inmates into groups to reduce the probability of assault and disruptive behavior. All inmates are classified using an objective classification process that at a minimum (a) Identifies the appropriate level of custody for each inmate; (b) Identifies appropriate housing assignment; (c) Identifies the inmate's interest and eligibility to participate in available programs. 4-ALDF-2A-30

Inmate management and housing assignment considers age, gender, legal status, custody needs, special problems and needs, and behavior. Male and female inmates are housed in separate rooms/cells. 4-ALDF-2A-32

Inmates are separated according to existing laws and regulations and/or consistent with the facility's classification plan. 4-ALDF-2A-33

Inmates not suitable for housing in multiple occupancy cells are housed in single occupancy cells. No less than ten percent of the rated capacity of the facility is available for single occupancy. 4-ALDF-2A-35

Confinement of juveniles under the age of 18 is prohibited unless required by state law. 4-ALDF-2A-37

If youthful inmates are committed to the facility, a plan is in place to provide for the following:

- supervision and programming needs of the youthful inmates to ensure their safety and security and education
- classification and housing plans
- appropriately trained program staff

4-ALDF-2A-38

The facility administrator or designee can order immediate segregation when it is necessary to protect an inmate or others. The action is reviewed within 72 hours by the appropriate authority. 4-ALDF-2A-44

When an inmate is transferred to segregation, health care personnel are informed immediately and provide assessment and review as indicated by the protocols established by the health authority. 4-ALDF-2A-45 (MANDATORY)

Segregation housing units provide living conditions that approximate those of the general inmate population. All exceptions are clearly documented. Segregation cells/rooms permit the inmates assigned to them to converse with and be observed by staff members. 4-ALDF-2A-51

All special management inmates are personally observed by a correctional officer at least every 30 minutes on an irregular schedule. Inmates who are violent or mentally disordered or who demonstrate unusual or bizarre behavior must be assessed by medical personnel, who will determine the supervision that is needed. All other inmates are personally observed by a correctional officer at least every 60 minutes on an irregular schedule. 4-ALDF-2A-52

PERFORMANCE STANDARD
2B. Physical force is used only in instances of self-protection, protection of the inmate or others, prevention of property damage, or prevention of escape.

Expected Practices

The use of physical force is restricted to instances of justifiable self-defense, protection of others, protection of property, and prevention of escapes, and then only as a last resort and in accordance with appropriate statutory authority. In no event is physical force used as punishment. 4-ALDF-2B-01 (MANDATORY)

Restraint devices are never applied as punishment. There are defined circumstances under which supervisory approval is needed prior to application. 4-ALDF-2B-02

Four/five point restraints are used only in extreme instances and only when other types of restraints have proven ineffective. Advance approval is secured from the facility administrator/designee before an inmate is placed in a four/five point restraint. Subsequently, the health authority or designee must be notified to assess the inmate's medical and mental health condition, and to advise whether, on the basis of serious danger to self or others, the inmate should is in a medical/mental health unit for emergency involuntary treatment with sedation and/or other medical management, as appropriate. If the inmate is not transferred to a medical/mental health unit and is restrained in a four/five point position, the following minimum procedures are followed:

- direct visual observation by staff is continuous prior to an assessment by the health authority or designee
- subsequent visual observation is made at least every 15 minutes
- restraint procedures are in accordance with guidelines approved by the designated health authority.
- all decisions and actions are documented

4-ALDF-2B-03 MANDATORY)

Procedures govern the availability, control, and use of firearms, less lethal devices, and related security devices, and specify the level of authority required for their access and use. Chemical agents and electrical disablers are used only with the authorization of the facility administrator or designee. 4-ALDF-2B-04

Written reports are submitted to the facility administrator or designee no later than the conclusion of the tour of duty when any of the following occur:

- discharge of a firearm or other weapon
- use of less lethal devices to control inmates
- use of force to control inmates
- inmate(s) remaining in restraints at the end of the shift 4-ALDF-2B-07

The use of firearms complies with the following requirements:

- weapons are subjected to stringent safety regulations and inspections.
- a secure weapons locker is located outside the secure perimeter of the facility
- except in emergency situations, firearms and unauthorized weapons are permitted only in designated areas to which inmates have no access
- employees supervising inmates outside the facility perimeter follow procedures for the security of weapons
- employees are instructed to use deadly force only after other actions have been tried and found ineffective, unless the employee believes that a person's life is immediately threatened
- employees on duty use only firearms or other security equipment that have been approved by the facility administrator
- appropriate equipment is provided to facilitate safe unloading and loading of firearms ALDF-2B-08 (MANDATORY)

PERFORMANCE STANDARD
2C. Contraband is minimized. It is detected when present in the facility.

Expected Practices

Procedures guide searches of facilities and inmates to control contraband and provide for its disposition. 4-ALDF-2C-01

A strip search of an arrestee at intake is only conducted when there is reasonable belief or suspicion that he/she may be in possession of an item of contraband. The least invasive form of search should be conducted. 4-ALDF-2C-03

A strip search of general population inmates is only conducted when there is reasonable belief that the inmate may be in possession of an item of contraband or when the inmate leaves the confines of the facility to go on an outside appointment or work detail. The least invasive form of search should be conducted. 4-ALDF-2C-04

Manual or instrument inspection of body cavities is conducted only when there is reasonable belief that the inmate is concealing contraband and when authorized by the facility administrator or designee. Health care personnel conduct the inspection in private. 4-ALDF-2C-05

PERFORMANCE STANDARD
2D. Improper access to and use of keys, tools and utensils are minimized.

Expected Practices

The use of keys is controlled. 4-ALDF-2D-01 (MANDATORY)

The use of tools and culinary equipment is controlled.
4-ALDF-2D-02 (MANDATORY)

Medical and dental instruments, equipment, and supplies (syringes, needles, and other sharps) are controlled and inventoried. 4-ALDF-2D-03 (MANDATORY)

3. ORDER
GOAL: Maintain an orderly environment with clear expectations of behavior and systems of accountability.

PERFORMANCE STANDARD
3A. Inmates comply with rules and regulations.

Expected Practices

Rules of inmate conduct specify acts prohibited within the facility and the range of penalties that can be imposed for various degrees of violation. 4-ALDF-3A-01

Disciplinary procedures governing inmate rule violations address the following:
- rules
- minor and major violations
- criminal offenses
- disciplinary reports
- pre-hearing actions/investigation
- pre-hearing detention
- an inmate is placed in disciplinary detention for a rule violation only after a hearing. 4-ALDF-3A-02

Policies governing supervision of female inmates by male employees and male inmates by female employees shall be based on equal employment opportunity and inmate privacy needs. Except in emergencies, facility employees shall not observe inmates of the opposite sex in toilet and shower areas. Adequate employees shall be available, as needed, to conduct or assist in the admissions process of female band male inmates, conduct searches of inmates, and perform other sensitive procedures involving inmates.

Inmates are permitted reasonable access to information in their own files and records. The facility administrator may restrict access to certain information, or provide a summary of the information, when its disclosure to the inmates presents a threat to individual safety and/or the security of the facility.

The detention facility shall be equipped with adequate self-contained breathing apparatus (SCBA), and all employees are trained in the use of the SCBA devices.

4. CARE

GOAL: Provide for the basic needs and personal care of inmates.

PERFORMANCE STANDARD

4C. Inmates maintain good health. Inmates have unimpeded access to a continuum of health care services so that their health care needs, including prevention and health education, are met in a timely and efficient manner.

Expected Practices

There is a written plan that addresses the protocol, treatment and management of infectious and communicable diseases as specified by the appropriate health authority. 4-ALDF-4C-14 (MANDATORY)

Management of bio-hazardous waste complies with applicable local, state and federal regulations. 4-ALDF-4C-18 (MANDATORY)

Intake medical screening for inmates commences upon the inmate's arrival at the facility and is performed by health-trained or qualified health care personnel. All findings are recorded on a screening form approved by the health authority. The screening should include:

Inquiry into:

- current medications
- current illness and health problems, including communicable and chronic diseases
- dental pain, swelling or functional impairment
- use of alcohol and other drugs including potential need for detoxification
- the possibility of pregnancy
- suicidal risk assessment
- cognitive or physical impairments

Observation of the following:

- behavior, including state of consciousness, mental status, appearance, conduct, tremor, and sweating
- body deformities and other physical abnormalities

- ease of movement
- condition of the skin, including trauma markings, bruises, lesions, jaundice, rashes, and infestations, recent tattoos, and needle marks or other indications of drug abuse

<u>Medical disposition of the inmate</u>:

- refusal of admission until inmate is medically cleared
- cleared for general population
- cleared for general population with prompt referral to appropriate health care service
- referral to appropriate health care service for emergency treatment 4-ALDF-4C-22 (MANDATORY)

A comprehensive health appraisal for each inmate is completed within 14 days after arrival at the facility, unless a health appraisal has been completed within the previous 90 days. 4-ALDF-4C-24 (MANDATORY)

Mental health services and activities are approved by the appropriate medical or mental health authority. 4-ALDF-4C-28

All inmates receive an initial mental health screening at the time of admission to the facility by mental health trained or qualified mental health care personnel. The mental health screening includes, but is not limited to:

<u>Inquiry into whether the inmate:</u>

- has a present suicide ideation
- has a history of suicidal behavior
- is presently prescribed psychotropic medication
- has a current mental health complaint
- is being treated for mental health problems
- has a history of inpatient and outpatient psychiatric treatment
- has a history of treatment for substance abuse

<u>Observation of:</u>

- general appearance and behavior
- evidence of abuse and/or trauma
- current symptoms of psychosis, depression, anxiety, and/or aggression

<u>Disposition of inmate</u>:

- cleared for general population
- cleared for general population with appropriate referral to mental health care service
- referral to appropriate mental health care service for emergency treatment 4-ALDF-4C-29 (MANDATORY)

A suicide prevention program is approved by the health authority and reviewed by the facility or program administrator. It includes specific procedures for handling intake, screening, identifying, and supervising of a suicide-prone inmate. All staff with responsibility for inmate supervision are trained on an annual basis in the implementation of the program. 4-ALDF-4C-32 (MANDATORY)

The health authority specifies all protocols and management of pharmaceuticals. 4-ALDF-4C-38 (MANDATORY)

PERFORMANCE STANDARD

4D. Health services are provided in a professionally acceptable manner. Staff are qualified, adequately trained, and demonstrate competency in their assigned duties.

Expected Practices

Clinical decisions are the sole province of the responsible clinician and are not countermanded by non-clinicians. 4-ALDF-4D-02 (MANDATORY)

Health-trained correctional and/or health care personnel respond to life threatening health-related situations within four-minutes unless staff safety would be compromised by the response. 4-ALDF-4D-08 (MANDATORY)

First aid kits are available in designated areas of the facility as determined by the designated health authority in conjunction with the facility administrator. 4-ALDF-4D-09

Involuntary administration of psychotropic medication(s) to inmates complies with applicable laws and regulations of the jurisdiction.
4-ALDF-4D-17 (MANDATORY)

The use of inmates for medical, pharmaceutical, or cosmetic experiments is prohibited. 4-ALDF-4D-18 (MANDATORY)

Health care encounters, including medical and mental health interviews, examinations, and procedures are conducted in a setting that respects the inmates’ privacy. 4-ALDF-4D-19

Only a medical or mental health professional may authorize the use of restraints for medical or psychiatric purposes. 4-ALDF-4D-21 (MANDATORY)

An investigation is conducted and documented whenever a sexual assault or threat is reported. 4-ALDF-4D-22-2

Sexual conduct between staff and detainees, volunteers or contract personnel and detainees, regardless of consensual status, is prohibited and subject to administrative and disciplinary sanctions. 4-ALDF-4D-22-5

Victims of sexual assault are referred under appropriate security provisions to a community facility for treatment and gathering of evidence.
4-ALDF-4D-22-6 (Mandatory)

Authorities having jurisdiction are immediately notified of an inmate's death. There is a protocol that describes actions to be taken in the event of the death of an inmate. 4-ALDF-4D-23

<u>PERFORMANCE STANDARD</u>
5C. The negative impact of confinement is reduced.

Expected Practices

Inmates have access to exercise and recreation opportunities. When available, at least one hour daily is outside the cell or outdoors. 4-ALDF-5C-01

Both outdoor and covered/enclosed exercise areas for general population inmates are provided in sufficient number to ensure that each inmate is offered at least one hour of access daily. Use of outdoor areas is preferred, but covered/enclosed areas must be available for use in inclement weather.

Segregation units have both outdoor and covered/enclosed exercise areas. The minimum space requirements for outdoor and covered/enclosed exercise areas for segregation units are as follow:

- group yard modules– 15 square feet per inmate expected to use the space at one time, but not less than 500 square feet of unencumbered space
- individual yard modules– 180 square feet of unencumbered space 4-ALDF-5C-04

<u>6. JUSTICE</u>

GOAL: Treat inmates fairly and respect their legal rights. Provide services that hold inmates accountable for their actions, and encourage them to make restitution to their victims and the community.

<u>PERFORMANCE STANDARD</u>
6A. Inmates' rights are not violated.

Expected Practices

Inmates are not subjected to personal abuse, corporal punishment, personal injury, disease, property damage or harassment.
4-ALDF-6A-07 (MANDATORY)

Inmates are allowed freedom in personal grooming except when a valid governmental interest justifies otherwise. 4-ALDF-6A-08

PERFORMANCE STANDARD

6B. Inmates are treated fairly.

Expected Practices

An inmate grievance procedure is made available to all inmates and includes at least one level of appeal. 4-ALDF-6B-01

There is no discrimination regarding administrative decisions or program access based on an inmate's race, religion, national origin, gender, sexual orientation, or disability. 4-ALDF-6B-02

When both males and females are housed in the same facility, available services and programs are comparable. 4-ALDF-6B-03

Inmates with disabilities, including temporary disabilities, are housed and managed in a manner that provides for their safety and security. Housing used by inmates with disabilities, including temporary disabilities, is designed for their use and provides for integration with other inmates. Program and service areas are accessible to inmates with disabilities who reside in the facility. 4-ALDF-6B-04

PERFORMANCE STANDARD

6C. Alleged rule violations are handled in a manner that provides inmates with appropriate procedural safeguards.

Expected Practices

There are written guidelines for resolving minor inmate infractions. Serious infractions are handled consistent with the requirements for limited due process. 4-ALDF-6C-01

When rule violations require formal resolutions, staff members prepare a disciplinary report that describes the alleged violation and forward it to the designated supervisor. 4-ALDF-6C-03

An inmate charged with a rule violation receives a written statement of the charge(s), including a description of the incident and specific rules violated. The inmate is given the statement at the same time the disciplinary report is filed with the disciplinary committee but no less than 24 hours prior to the disciplinary hearing. The hearing may be held in less than 24 hours, only with the inmate's written consent. 4-ALDF-6C-07

Inmates charged with rule violations are present at the hearing, unless they waive that right in writing or through behavior. Inmates may be excluded during testimony. An inmate's absence or exclusion is documented. 4-ALDF-6C-08

7. ADMINISTRATION AND MANAGEMENT

GOAL: Administer and manage the facility in a professional and responsible manner, consistent with legal requirements.

PERFORMANCE STANDARD

7B. Staff, contractors, and volunteers demonstrate competency in their assigned duties.

Expected Practices

A criminal record check is conducted on all new employees, contractors, and volunteers prior to their assuming duties to identify those who should not be allowed to work in the facility. 4-ALDF-7B-03

Each employee is provided with an orientation prior to assuming duties. (See appendix for suggested topics)

- working conditions
- code of ethics
- personnel policy manual
- employees' rights and responsibilities
- overview of the criminal justice system
- tour of the facility
- facility goals and objectives
- facility organization
- staff rules and regulations
- personnel policies
- program overview 4-ALDF-7B-05

All professional, support, clerical, and health care employees, including contractors, receive continuing annual training. (See appendix for suggested topics) security procedures and regulations

- supervision of inmates
- signs of suicide risk
- suicide precautions
- use-of-force regulations and tactics
- report writing
- inmate rules and regulations

    - key control
    - rights and responsibilities of inmates
    - safety procedures
    - all emergency plan and procedures
    - interpersonal relations
    - social/cultural lifestyles of the inmate population
    - cultural diversity
    - communication skills
    - CPR/First aid
    - counseling techniques
    - sexual harassment/sexual misconduct awareness
- the purpose, goals, policies and procedures for the facility and parent agency; security and contraband regulations
- key control
- appropriate conduct with inmates
- responsibilities and rights of employees
- universal precautions
- occupational exposure
- personal protective equipment
- bio-hazardous waste disposal
- an overview of the correctional field 4-ALDF-7B-08

Prior to assuming duties, all correctional officers receive training in the facility under the supervision of a qualified officer. At a minimum, this training covers the following areas:

- facility policies and procedures
- suicide prevention
- use-of-force
- report writing
- inmate rules and regulations
- key control
- emergency plans and procedures
- cultural diversity
- communication skills
- cardiopulmonary resuscitation (CPR)/first aid
- sexual misconduct

In each subsequent year of employment correctional officers receive documented in-service training in critical areas of the operation. 4-ALDF-7B-10

All personnel authorized to use firearms and less lethal weapons must demonstrate competency in their use at least annually.
4-ALDF-7B-15 (MANDATORY)

Detailed training records must be maintained for each employee. The facility must keep an archive of all training material/programs provided to employees.

PERFORMANCE STANDARD
7C. Staff, contractors, and volunteers are professional, ethical and accountable.

Expected Practices

The facility and administration affirm support for a drug-free workplace for all employees. 4-ALDF-7C-01

The facility has a written code of ethics that it provides to all employees. 4-ALDF-7C-02

PERFORMANCE STANDARD
7D. The facility is administered efficiently and responsibly.

Expected Practices

Written policies and procedures describe all facets of facility operation, maintenance, and administration and are reviewed annually. 4-ALDF-7D-06

New or revised policies and procedures are disseminated to staff, and, where appropriate, to contractors, volunteers, and inmates, prior to implementation. 4-ALDF-7D-08

The facility administrator prepares and submits an annual budget that requests necessary resources for facility operations and programs. 4-ALDF-7D-10

PERFORMANCE STANDARD
7F. The facility is a responsible member of the community.

Expected Practices

Each volunteer completes an appropriate, documented orientation and/or training program prior to assignment. The lines of authority, responsibility, and accountability for volunteers are specified. 4-ALDF-7F-05

APPENDIX K: Step-By-Step Guide to Using the EASI Program

A. Instructions for Using the *EASI Simplified Version*

The EASI program (Estimate of Adversarial Sequence Interruption) is an analytical tool that offers new insights and opportunities for corrections. The EASI program is operated using Microsoft Excel software. Section II-I of the *Corrections Vulnerability Handbook* describes some of the analytical powers of the EASI program. This appendix describes how to open and navigate the program.

Two versions of the EASI program have been adapted for use in Correctional Vulnerability Assessments (CVA):

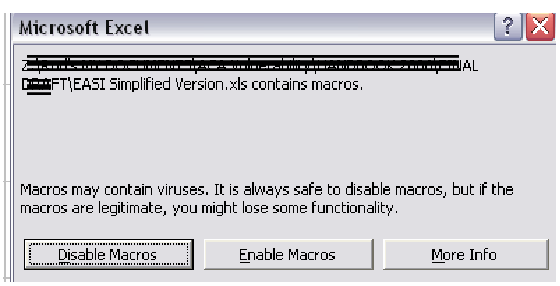
- EASI Simplified Version
- EASI Advanced Version

This narrative will describe the methods for using the EASI Simplified Version and then provide additional instructions for using the complete version.

1. Opening the EASI Program

When you first open the EASI program you will encounter a box that asks:

Figure 1: Excel Warning Message



Click on the button “Enable Macros” in order to proceed.

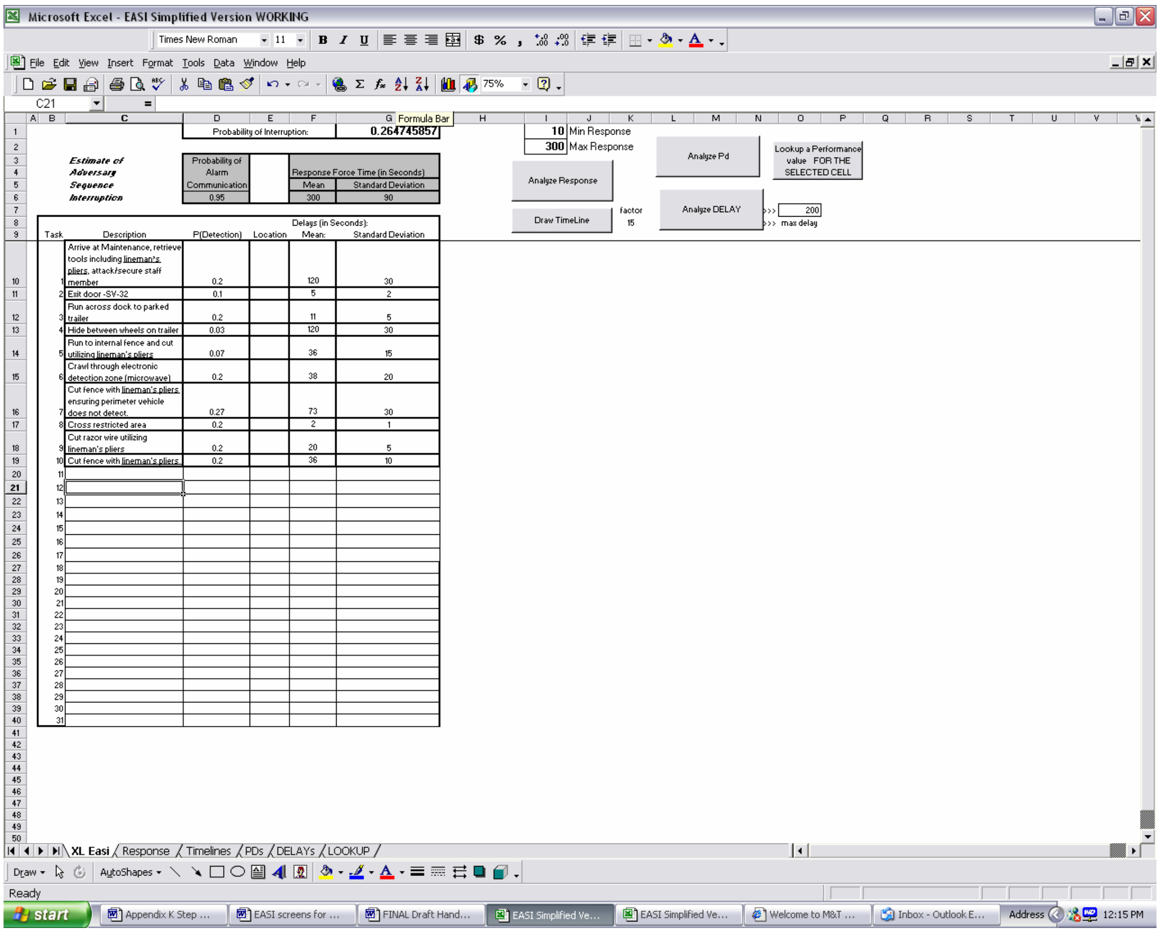
2. Navigating on the “XL EASI” Worksheet

The EASI program will open on the worksheet entitled “XL EASI” which is labeled on the tab at the bottom left of the page.

Other tabs identify additional worksheets that will be used to analyze scenarios and to lookup values for delay elements. These tabs are:

- Response
- Timelines
- PDs
- Delays
- Lookup

Figure 2: Initial Screen for XL EASI Worksheet



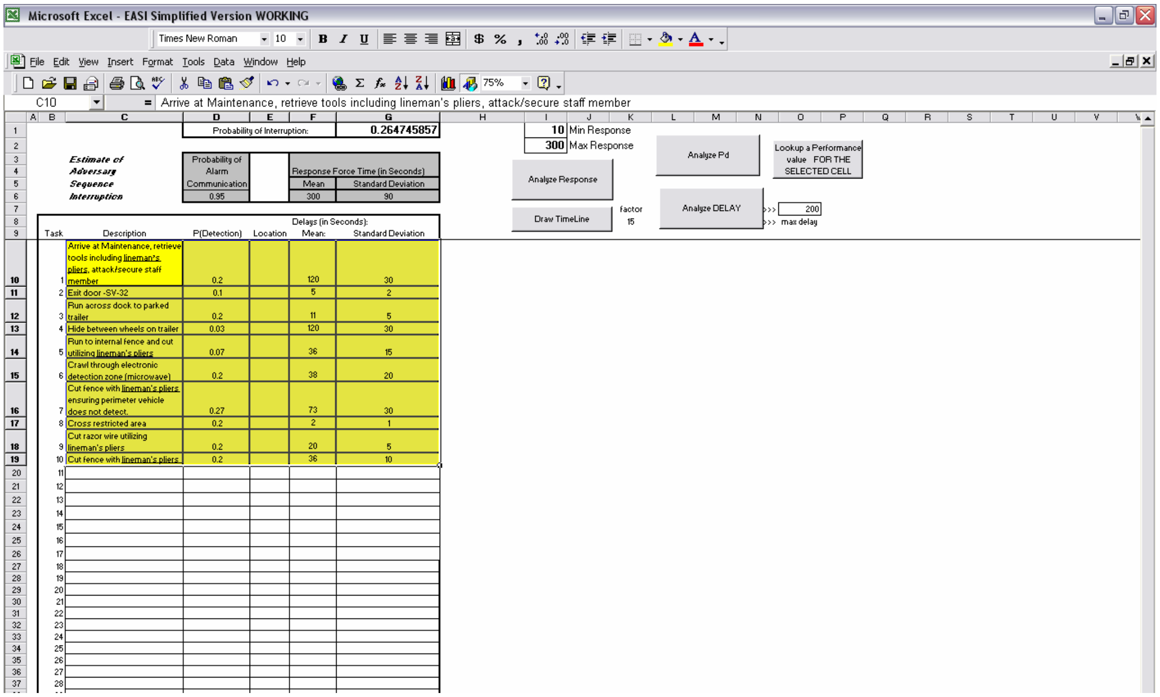
This is your "home page" for using EASI in its simplified form.

3. Clearing the Sample Scenario

Row 9, columns A through G has the headings for the scenario that you will be entering for evaluation. A sample scenario is provided.

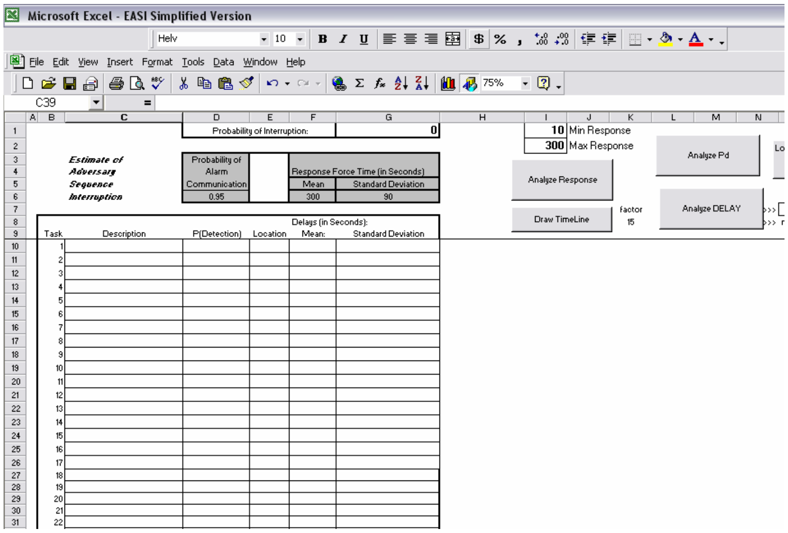
To evaluate a new scenario, highlight all of the cells from Row 10 to the bottom of the table (see Figure 3.)

Figure 3: Highlighting the Table Prior to Clearing It



Then press “delete” to clear the text. This will clear the EASI table for you to enter your own data and information. It should now look like the example in Figure 4.

Figure 4: EASI Table Cleared and Ready for Data Entry



4. Entering Data for Your Scenario

Using the table that you have cleared, enter the information and data for your scenario. If you created a table such as the one in Figure 5 prior to opening EASI, you should be able to paste it into the EASI table. If not, you will need to type it in on the Excel spreadsheet.

Figure 5: Scenario Table

				Delays (in Seconds):	
Task	Description	P(Detection)	Location	Mean:	Standard Deviation
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					
11					
12					
13					
14					
15					
16					

"Description" refers to the specific task or step in the scenario, such as "cut the fence with pliers".

"Location" refers to the point in each step at which detection occurs, and should be entered as:

- B (for Beginning)
- M (for Middle)
- E (for End)

<u>Tip:</u> If you have not determined the location, you may leave this column blank and EASI will still work. You may also enter "M" as the value for all of the steps, as in the sample that has been provided.

Figure 6 shows the table filled in for the sample scenario. This is the scenario that is described in the handbook as Figure II.30 in Section II.I.

Figure 6: Sample Scenario (see Figure II.30 in Handbook)

				Delays (in Seconds):	
Task	Description	P(Detection)	Location	Mean:	Standard Deviation
1	Arrive at Maintenance, retrieve tools including lineman's pliers, attack/secure staff member	0.2		120	30
2	Exit door -SV-32	0.1		5	2
	Run across dock to parked trailer	0.2		11	5
4	Hide between wheels on trailer	0.03		120	30
5	Run to internal fence and cut utilizing lineman's pliers	0.07		36	15
6	Crawl through electronic detection zone (microwave)	0.2		38	20
7	Cut fence with lineman's pliers ensuring perimeter vehicle does not detect.	0.27		73	30
8	Cross restricted area	0.2		2	1
9	Cut razor wire utilizing lineman's pliers	0.2		20	5
10	Cut fence with lineman's pliers	0.2		36	10

Note that the sample above has no values for the "location" column. EASI will work without this variable, but your results will be more accurate if you are able to enter values (B,M or E) for this field.

6. Understanding the Probability of Interruption (P_I)

The bottom line output for the EASI program is $\mathbf{P_I}$. This tells you the odds that you will interrupt, or stop, an inmate before he/she is successful. A low P_I means that you are less likely to stop the event. You may use EASI to help you identify ways to increase the P_I by changing:

- response force time
- probability of detection
- length of delay

The P_I value for the scenario that is shown on your screen is in the upper part of the XL EASI worksheet, as shown in Figure 7.

Figure 7: Probability of Interruption

Probability of Interruption:	**0.264745857**

Estimate of Adversary Sequence Interruption

Probability of Alarm Communication	Response Force Time (in Seconds)	
	Mean	Standard Deviation
0.95	300	90

In the example in Figure 7, the probability of interruption is 0.26475857. Put another way, this means that you could expect to successfully stop an inmate 26 times out of 100 attempts.

If you change any of the values in the scenario table, or the response time, P_I will automatically be recalculated.

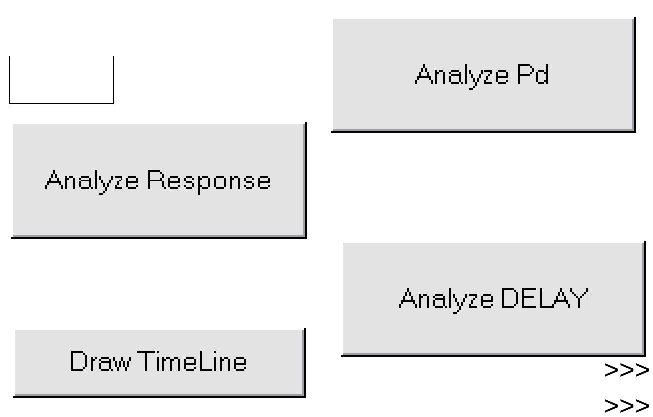
<u>TIP</u>: As you experiment with different values for detection, delay and response, you may use the "undo" arrow to go back to your previous value. This makes it easy to experiment without losing the original material.

<u>TIP:</u> If you want to save a variation for future analysis, you should click on "File" and then "Save As" and rename the file. Remember that the new name will stay with the file until you change it again.

7. Analyzing Detection, Delay and Response

Instead of using a "trial and error" approach to determine the impact of changes in detection probabilities, delay, or response time, try using the buttons on the top of the EASI worksheet.

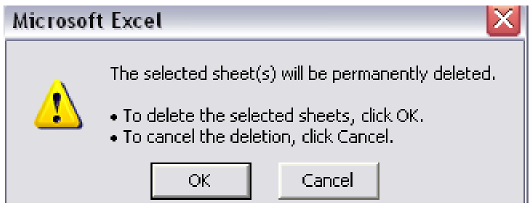
Figure 8: Analytical Buttons



Drawing a Timeline

Making a graphic image of the timeline is a good starting point for your analysis of the scenario. If you click on the "draw timeline" button you will be taken to another worksheet. But before you may use that worksheet, you have to respond to an Excel query that tells you that the selected sheet will be permanently deleted, and asks your permission to proceed.

Figure 8: Excel Query to Create Timeline



Click on "OK." All you are doing is erasing the old timeline so that the new on may be drawn.

After you click on "OK" a new timely will be drawn. It provides a graphic view of the timeline of activities associated with your current scenario.

TIP: If you want to save a timeline, click on the far upper right corner of the worksheet. This will select everything on the sheet. Then click on "Edit" and then "Copy." Click on "Insert" and then "Worksheet" and you will be taken to a new blank worksheet. Click on "Edit" and then "Paste" and the timeline will be copied to the new sheet. If you click on the tab at the bottom you will be able to assign a new name to the sheet. This will save a picture of the timeline with the rest of your EASI file.

Analyzing Response

If you click on the "Analyze Response" button it will take you to another worksheet, such as the one shown in Figure 9.

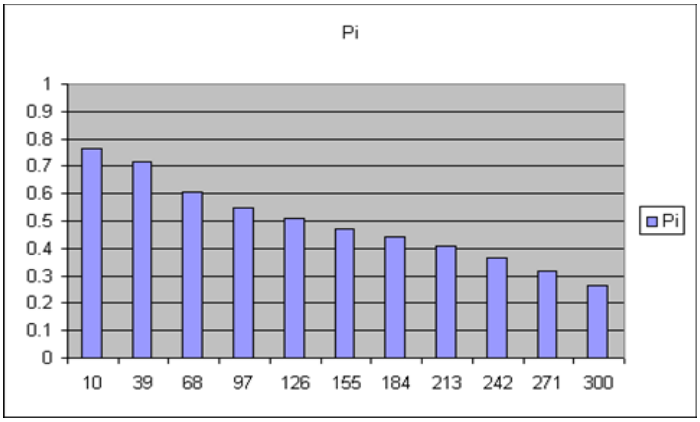
The figures in the column labeled "Response Time" represent hypothetical changes in response time. In the next column the corresponding P_I value for each response time. For example, if response time is changed to 68, the P_I would be 0.606675995.

The graph shows this relationship between P_I and response time.

Using this information, you may be able to set a new target for response time that provides the most payoff in terms of stopping inmates effectively.

Figure 9: Analyzing Response

Response Time	Pi
10	0.765209862
39	0.717203547
68	0.606675995
97	0.548871413
126	0.507606661
155	0.472696643
184	0.441396418
213	0.406832948
242	0.364369734
271	0.315356922
300	0.264745857

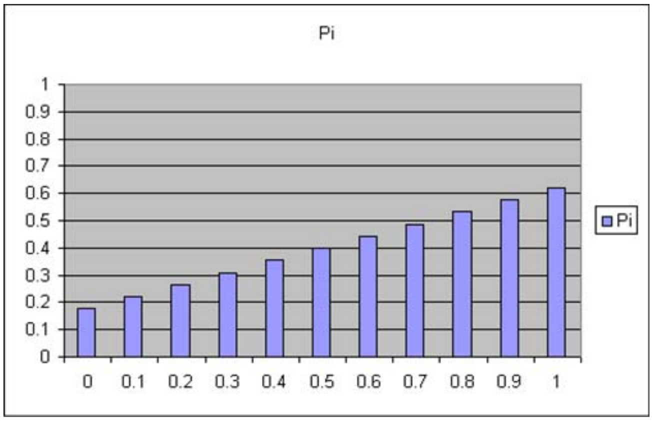


Analyzing Probability of Detection

Before you use the "Analyze Detection" button you have to select a cell to be analyzed but clicking on it. If you click on the first P_D value in the table, and then on the button, you will get a new worksheet with values and a chart. If you forget to select a value, Excel will remind you with a prompt.

Figure 10: Analyzing Detection

PD	Pi
0	0.175555608
0.1	0.220150732
0.2	0.264745857
0.3	0.309340981
0.4	0.353936106
0.5	0.39853123
0.6	0.443126355
0.7	0.487721479
0.8	0.532316604
0.9	0.576911729
1	0.621506853



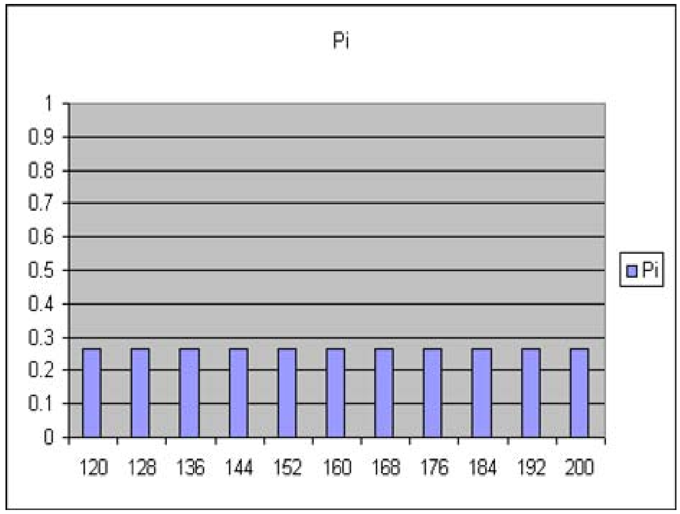
The table will tell you the impact of changes in P_D on the probability of interruption, and the graph shows the relationship. For example, if you increase P_D to 0.5 the probability of interruption will increase to 0.443. You may reverse the process and select a probability of interruption that is acceptable and find the corresponding P_D necessary to achieve your goal.

Analyzing Delay

The “Analyze Delay” button works the same way as the detection button-- select a value by clicking on a cell in the delay column, and then click on the button.

Figure 11: Analyzing Delay

DELAY	Pi
120	0.264745857
128	0.264745857
136	0.264745857
144	0.264745857
152	0.264745857
160	0.264745857
168	0.264745857
176	0.264745857
184	0.264745857
192	0.264745857
200	0.264745857



As with detection and response time, you may use the table and the graph to analyze changes in delay. But in this example, changing delay does not make a difference! This is also good information because it helps you to focus on PPS elements that will have the greatest impact.

8. Using the “Lookup” Function for Delay Values

“Lookup” is another tool that is embedded in the EASI program allows you find how long certain PPS elements delay an action.

The data contained in the lookup function was developed by Sandia National Laboratories several years ago. This information should be used as a last resort only, for several reasons:

- It was not initially developed for applications in corrections
- It is not current with the newest technology
- Data that you develop yourself on-site will always be more meaningful.

The drop-down menus allow you to select the type of safeguard class, type, and description. When you do this, four different delay values (measured in seconds) will be shown at the top of the worksheet, corresponding to the equipment and materials that might be available to the inmate.

Figure 12: "The Lookup" Function

	DELAY				
	No Equipment	Hand Tools	Power Tools	High Explosives	
double click to copy this value->	30000	240	180	45	
Safeguard Class:					
Access Delay					
Safeguard Type:					
Bag Port Cover					
Description					
1/4 inch steel					

Appendix G of the handbook contains all of the information that is inside the lookup function, as a long series of tables.

Summary

Using the simplified version of EASI you are able to examine each element of the scenario, enter new values, and immediately determine the impact on the probability of interruption.

This will lead you to the critical element(s) that could reduce risk if you can find a way to change the detection, delay or response.

B. Instructions for Using the *Advanced EASI Version*

There is a more advanced version of EASI available to those who have the need and the confidence to try it. The advanced program is different from the simplified version because:

- It starts with a complete ASD (adversary sequence diagram) that describes all elements the PPS and facility
- It analyzes the ASD and creates *all* of the potential pathways and calculates the corresponding probability of interruption

The advanced EASI version is actually contained in the simplified version, but it is hidden.

To reveal the advanced EASI worksheets:

1. Click on “Format”
2. Click on “Sheet”
3. Click on “Unhide”
4. Click on “Multipath Inputs”

A large colored screen will appear, which is the multipath input worksheet. You will need to repeat the steps above and click on “Results” to reveal the second worksheet that is part of the advanced EASI program.

A. The Multipath Input Worksheet

The sample that is in the multipath input worksheet is based on an assault on a nuclear power installation, with the goal of stealing an “asset” such as radioactive materials.

The multipath worksheet describes all of the potential steps and tasks that have been identified for assaulting the facility. The detection and delay values are entered for each.

Before attempting to clear the data on the worksheet so that you may enter new values, you should have a complete ASD in hand that shows all of the PPS elements, facility features, and corresponding delay and detection values.

Figure 13 shows the worksheet that you have revealed on your EASI program. It describes all of the *potential* ways to assault the facility, rather than asking you to select only one path for analysis.

Entering your own ASD into this worksheet will be arduous and challenging. But if you are successful, you will discover expanded value from the EASI program.

Figure 13: The Multipath Worksheet

				Lookup a Performance value FOR THE SELECTED CELL
Alarm Communication		0.95		
Response Force Time	Mean	300		
	Std Dev	90		
	Areas	Name		
	1	Outside		
	(B,M,E)	(B,M,E)		Element Name
Detection	P_D	XXX		(B,M,E)
	Desc	XXX	Detection	P_D
Delay	Mean	XXX		Task Description
	Std Dev	XXX	Delay	Mean
DBL-click to DELETE AREA below		double-click here to shift data down for new area		Std Dev
				Jump to Area
	2	Limited Area		
	(B,M,E)	B		Element Name
Detection	P_D	0		(B,M,E)
	Desc	run to ISO zone	Detection	P_D
Delay	Mean	200		Task Description
	Std Dev	50	Delay	Mean
DBL-click to DELETE AREA below		double-click here to shift data down for new area		Std Dev
				Jump to Area
	3	Protected Area		
	(B,M,E)	B		Element Name
Detection	P_D	0		(B,M,E)
	Desc	run to building	Detection	P_D
Delay	Mean	12		Task Description
	Std Dev	3.6	Delay	Mean
DBL-click to DELETE AREA below		double-click here to shift data down for new area		Std Dev
				Jump to Area

As with the XL EASI worksheet, you may use the “lookup” function by pressing the button at the top of the screen.

When you have completed all of the entries for the multipath worksheet, press the "Process Paths" button at the top of the screen. This will prompt EASI to look at all of the possible paths that may be navigated.

B. The Results Worksheet

Once you have processed the results, you will be able to review them on the "Results" worksheet. This sheet presents every possible combination and permutation of paths to accomplish the objective, and a probability of interruption for each. EASI will present the paths in order of increasing P_I so that the most vulnerable ones will be at the top.

Figure 14: The Multipath Worksheet

		Double Click on 'Path:X'				
Pi	**TRI**					
0.2659	**30**	**Path: 15**	Element: Helicopter (fly in to protected area) [(0.02) M 60/20]	**Area: Protected Area (run to building) [(0) B 12/3.6]**	Element: Surface (come through wall) [(0.9) E 90/27]	Area: Building (run to vital area) [(0) B 10/3]
0.4018	**-60**	**Path: 13**	Element: Helicopter (fly in to protected area) [(0.02) M 60/20]	Area: Protected Area (run to building) [(0) B 12/3.6]	**Element: Door (open door) [(0.5) B 90/27]**	Area: Building (run to vital area) [(0) B 10/3]
0.4324	**20**	**Path: 14**	Element: Helicopter (fly in to protected area) [(0.02) M 60/20]	Area: Protected Area (run to building) [(0) B 12/3.6]	Element: Door (open door) [(0.5) B 90/27]	**Area: Building (run to vital area) [(0) B 10/3]**
0.4807	**30**	**Path: 3**	Element: Fence (cut fence) [(0.02) B 10/3]	Area: Limited Area (run to ISO zone) [(0) B 200/50]	Element: Vehicle Portal (open gates) [(0.5) M 40/27]	**Area: Protected Area (run to building) [(0) B 12/3.6]**
0.4807	**30**	**Path: 11**	Element: Fence (cut fence) [(0.02) B 10/3]	Area: Limited Area (run to ISO zone) [(0) B 200/50]	Element: ISO zone (cross ISO zone) [(0.5) M 40/27]	**Area: Protected Area (run to building) [(0) B 12/3.6]**
0.5274	**20**	**Path: 16**	Element: Helicopter (fly in to protected area) [(0.02) M 60/20]	Area: Protected Area (run to building) [(0) B 12/3.6]	Element: Surface (come through wall) [(0.9) E 90/27]	**Area: Building (run to vital area) [(0) B 10/3]**
0.5487	**-60**	**Path: 1**	Element: Fence (cut fence) [(0.02) B 10/3]	Area: Limited Area (run to ISO zone) [(0) B 200/50]	Element: Vehicle Portal (open gates) [(0.5) M 40/27]	Area: Protected Area (run to building) [(0) B 12/3.6]

0.5487	**-60**	**Path: 9**	Element: Fence (cut fence) [(0.02) B 10/3]	Area: Limited Area (run to ISO zone) [(0) B 200/50]	Element: ISO zone (cross ISO zone) [(0.5) M 40/27]	Area: Protected Area (run to building) [(0) B 12/3.6]
0.6459	**20**	**Path: 2**	Element: Fence (cut fence) [(0.02) B 10/3]	Area: Limited Area (run to ISO zone) [(0) B 200/50]	Element: Vehicle Portal (open gates) [(0.5) M 40/27]	Area: Protected Area (run to building) [(0) B 12/3.6]

Each potential path has been assigned a number, in the third column. The P_I is shown in the first column. The steps in the path are shown in the columns to the right.

Now you have the full range of potential paths available for analysis. Pick a path by double clicking on the cell in the third column (to select Path 16 click on that cell.) This will prompt EASI to past the path into the scenario table on the XL EASI worksheet so that you may analyze it in more detail. You will be taken to that worksheet automatically.

Summary

Using the advanced features of EASI will be difficult, but if you are able to work your way through the process, you will have a more potent and flexible analytical tool.

Appendix L: Sample CVA Report[1]

Vulnerability Analysis
_____________ Department of Corrections
State Correctional Institution at ___________
February 1 through 5, 2003

Insert Picture of Facility

Report prepared by:

Chris Robertson

Final Report: Date

Prepared at _____________

This document is considered "Corrections Confidential" and is not public information. It shall not be released in its entirety or in part without the approval of the ___________ Secretary of Corrections or its designee. It may be released to any ___________ Department of Corrections employee on an as-needed basis.

_______ Department of Corrections

[1] Source: Sandia National Laboratories

Acknowledgments

Sponsor

The ___________ Department of Corrections performed this Vulnerability Analysis (VA) under the direction of the Secretary of Corrections _________________.

Team Members

List all team members Location

Chris Robertson, Sandia National Laboratories

____________ *Department of Corrections Comments*

The Vulnerability Team extends its appreciation to Superintendent ______________ and his/her staff for their courtesy, cooperation and assistance during this analysis.

Table of Contents

ACRONYMS

ABSPO	activation by sally port officer
CI	correctional industries
CO	correctional officer
CRO	control room officer
E	end
EASI	Estimate of Adversary Sequence Interruption
H	high
L	low
M	medium
MW	microwave
P_D	probability of detection
P_I	probability of interruption
P_N	probability of neutralization
PPS	physical protection system
PSD	path sequence diagram
PTZ	pan/tilt/zoom
RF	response force
RFT	response force time
RHU	restricted housing unit
SCI	State Correctional Institution
SNL	Sandia National Laboratories
TL VCR	time-lapse videocassette recorder
VA	vulnerability analysis
OBG	observation by guard
Snw	sensor not working
MWnw	microwave not working
OBT	observation by tower
VO	video observation
OBS	observation by staff
OBOSP	observation by outside security patrol
EO	expert opinion

Executive Summary

The __________ VA Team conducted a Vulnerability Analysis (VA) at ___________ on February 1, 2003 through February 5, 2003.

The ___________ VA Team's stated objectives were to_______________________ ____ ____ ____________________.

One page summary of what you found. This summary should be a stand alone page.

Project Description

The __________ VA Team conducted a Vulnerability Analysis (VA) at __________ during the week of February 1 to 5, 2003. The team consisted of prison security experts from various _________ facilities and two technical experts in security hardware.

A *vulnerability analysis* is a systematic evaluation in which quantitative and/or qualitative techniques are applied to determine the physical protection system's effectiveness level against specific undesired events and/or a range of potential threats. The undesired events and potential threats are contained in a Vulnerability Assessment Threat Statement that was developed by _________ subject matter experts and is located in Appendix B. The two highest priorities are preventing (1) inmate escapes and (2) the introduction of contraband.

Process

The _______ VA Process consists of the following tasks:

1. _______ management selects two team leaders to conduct the VA and assigns a team of prison security experts from various _______ facilities to the task.
2. The VA Team Leaders visit the site to conduct a preliminary meeting with the facility's management to understand and define the project objectives and to become acquainted with the facility's policies, procedures, and areas of concern.
3. The VA Team members meet at the facility and participate in a team orientation, read the policies and procedures, and become familiar with the facility's characteristics. The facility also provides areas of concern that the facility would like to have evaluated for vulnerabilities.
4. The VA Team leaders assign tasks and roles to the team members.
5. The VA Team members disperse throughout the site and observe the areas and complete their tasks.
6. The VA Team gathers together and discusses their observations, writes the observations, and creates updated path sequence diagrams that describe how inmates could defeat the security systems.
7. The VA Team defines the scenarios that could result in inmate escapes or the introduction of contraband.
8. The VA Team conducts a limited scope exercise to test specific features of the Physical Protection system and to gather additional pertinent information. The objective is to simulate parts of the scenario and to attempt to defeat the security system in selected vulnerable areas without interrupting prison security or safety requirements.
9. The VA Team analyzes the results of the scenarios.

The team visited SCI _______ and conducted the VA, starting with a characterization of the facility and the operational conditions. Superintendent _______ and the Executive Staff requested the VA team focus on the procedures used at entrance and exit points to uncover the potential ability to introduce contraband and/or the potential for unauthorized egress from the facility at the following areas:

- Sally Port—Vehicles entering and exiting the facility
- ____
- ______________________________________

Summary of the Process

During the VA process, the team characterized the facility, assessed the threats, identified the undesired events, described and analyzed the existing physical protection system (PPS), ran limited scope performance tests, and identified potential vulnerabilities and associated risk.

Facility Overview

Facility Description and Operational Condition

The State Correctional Institution at ________ is a Security Level _, _________-security adult male facility located in ____________________. SCI-________ is situated on ____ acres. There are __ acres enclosed within the perimeter.

SCI-________'s current bed capacity is 2,425.

Locations that were visited during the VA

General Population Housing Units
Level 5 Housing Unit
Visiting Room
Yard/Field House
Front Gate/Staff Entrance
____
____

Sally Port
Control Center
Dietary
Power Plant
Laundry/Shoe Shop/Clothing Exchange

Procedures and Operations that were reviewed during the VA

- Key Control
- Tool Control
- Inmate Accountability Practices
- Vehicle Procedures
- Staff and Visitor Search Procedures
- Inmate Accountability
- Perimeter detection and delay
- ____________________________

Scenarios

Escape Scenarios

The following worst-case escape scenarios were identified:

Scenario #1 – Loading Dock to Sally Port:
Simulated test conditions: clear skies, nighttime, full complement of staff
Tools necessary: ______________________________

____.

Analysis of Scenario #1
____

Include Picture wherever possible
Figure 1. ***Figure 2.***

Figure 3. ***Figure 4.***

Scenario #2 – Escape using

Simulated test conditions: clear skies, daytime, full complement of staff
Tools necessary: ________________

Describe Scenario in detail

Analysis of Scenario #2

Report what the analysis concludes including what risk the facility is at. Facility is at **high risk** for completion of this scenario. (Refer to ______). (Recommended enhancements, refer to _________)

Scenario #3 ____

Contraband Scenarios

The following two worst-case scenarios were identified for the introduction of contraband.

Scenario #1 ____.

Scenario #2 – ____

Analysis of Contraband Scenarios:
____

Perimeter and Other Major Areas of Interest

Perimeter Description

The perimeter surrounding SCI – _______ consists of _____________' fences approximately __' apart. Both fences are constructed of ___gauge security grade diamond mesh wire on the lower half and security grade anti-climb on the upper half. The inner fence is equipped ____
____
____
____.

One OSP is on duty on the 0600 to 1400 and 1400 to 2200 shifts. The 2200 to 0600 shift has two OSPs on duty. The OSP is armed with a _____ caliber revolver After ___ hours, the Inside Patrol Officer relieves this post.

All alarms report to the Video Monitoring Station in Central Control. Fence vibration alarms also report to ________________.

Perimeter Testing

On 12-02-03 the Team conducted performance tests on ____

Include Pictures

Figure 9 _______________ ***Figure 10*** ______________

Recommendations for the Perimeter Intrusion Detection System:

The Team recommends the SCI-_______ conduct and record quarterly performance tests of all zones by the Maintenance Department and install ___

Video System Description

Video monitoring and surveillance at SCI-_______ is supported by __________________

Observations and Recommendations Regarding Video System:

The Team observed that video assessment of perimeter alarms is ________

Vehicle Sally Port

The Sally Port is located at the north east side of the facility. This area is staffed by one sergeant Monday through Friday during the hours of 0730 through 1530. The Sally Port has two sliding vehicle gates and two personnel gates. All gates are remotely controlled from Central Control through voice command over an intercom system. The gates are interlocked electrically with an override feature for emergencies. The sergeant and Central Control have video monitoring capabilities of ____ cameras placed at the Sally Port. One camera is placed watching the desk and weapons storage area for Central Control to monitor activity. The sergeant has keys to the building and the weapons storage cabinets. Inmates and staff are processed into the institution utilizing a walk-through and hand-held metal detector. Other staff at a predetermined location inside the institution conducts any random strip searches of inmates reentering the institution. All vehicles are searched coming into or leaving the institution. Weapons are locked in ____________.

The delay and detection equipment at the Sally Port consists of gates, fences, razor wire, __________________..

Observations and Recommendations Regarding the Sally Port:

The Sally Port has ___________________. The fence fabric at the Sally Port is secured in a manner that would allow opportunity for disassembly. The team recommends:

- ___________________________________.
- ____________________________________

Main Exercise Yard Description

SCI-_______ has two Main Exercise Yards located at the east side of the facility. Entrance into the yards is through a pedestrian slam gate, staffed by an officer during yard activity responsible for monitoring inmate movement into and out of the Yard. One Commissioned Officer supervises activity in both Yards. One Sergeant and four Corrections Officers staff each Yard. A tower is located outside the secure perimeter on the east side of the facility staffed by a Corrections Officer during Yard activity. This officer is armed with a ____ caliber rifle and ____ shotgun. A 14' 6-gauge security grade diamond mesh fence separates the Yards. Each yard consists of a ¼ mile track, softball field, bleachers, tables, bocce ball court, weight pavilion, and free weight area.

Key Observations and Recommendations

List approximate 10 (maximum) key observation that support why the scenarios are potentially successful.

1. Inmate Accountability – Pass control and inmate accountability is________

2. Key Control –.

3. Detection and Delay at Sally Port –.

4. Internal Officer Response –

5. Outside Perimeter Response –.

6. Main Exercise Yard Observations

7. Camera Placement – ____________________ The VA Team recommends institutional review.

8. Visitor Exit Procedures –

9. etc

Analysis

The results of the VA include worst-case scenarios, relative risk calculations, observations made during the assessment, and recommendations to decrease the risk for both escape and the introduction of contraband.

The VA _______ team made the following list of limitations and assumptions:

1. Limited performance testing data was used when available, but sufficient data was not available to accurately define each physical protection element. Data was gathered in an effort to accurately define the probability of detection, delay times, and response force times using the best available resources. Due to the limited amount of data available at the time of the assessment, conclusions were drawn using a combination of first-hand observation and expert opinion.
2. The mean time for delay times and the probability of detection data were based on expert opinion and similar data when the information was not readily available. The standard deviation was estimated to be 20% in all cases where the testing has not been done and data was not available. The probability of detection and delay times were estimated in the favor of the inmate when accurate data were not available in order to make conservative estimates and emphasize security.
3. All DOC procedures are assumed to be conducted in accordance with established policies and to be effective except where noted.
4. A tabletop methodology using expert opinion and predetermined goals identified by the institution was used to identify escape and contraband paths. These paths were evaluated using Path Sequence Diagrams (PSDs) and Estimate of Adversary Sequence Interruption (EASI).
5. Levels of acceptable risk were not determined.
6.

There was not enough time for the team to analyze every path in detail during the one-week VA. The process used to determine the worst-case scenarios was as follows:

- ➢ Map out a PSD for all areas of concern for escape and the introduction of contraband.
- ➢ Refine the detection and delay path elements to include testing data where possible.
- ➢ Use the PSD to determine the mathematical worst-case paths.
- ➢ Develop a cohesive, logical, credible scenario for the worst-case paths.
- ➢ Use EASI to evaluate the paths with the lowest probability of detection and/or shortest timelines.
- ➢ Use the risk equation to determine the worst-case scenarios that put the institution at the highest risk.

- All of the paths were developed and evaluated for specific conditions.

Escape strategies are also an important consideration. These strategies include:

- An inmate could wait until he was permitted out of his cell and initiate the escape from another location or while he was transitioning from one area to another, or

- An inmate could use violence to force his way out.

Using these escape approaches, the team developed PSDs with starting points initiated at the cell, workplace area, and the restricted area (assuming after potentially years of planning an inmate could find a way to start as far out as the restricted area without being detected).

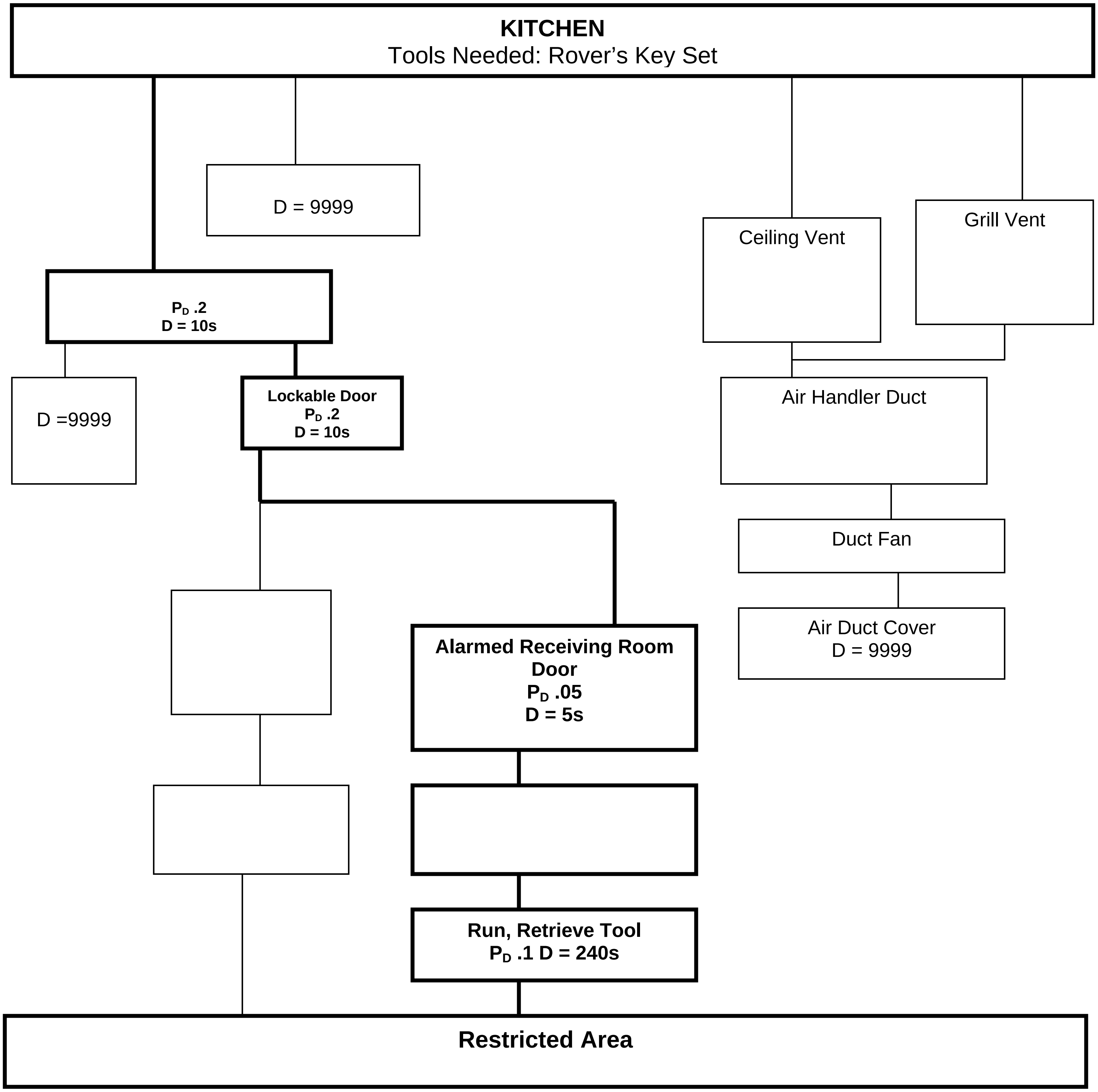
Path Sequence Diagrams

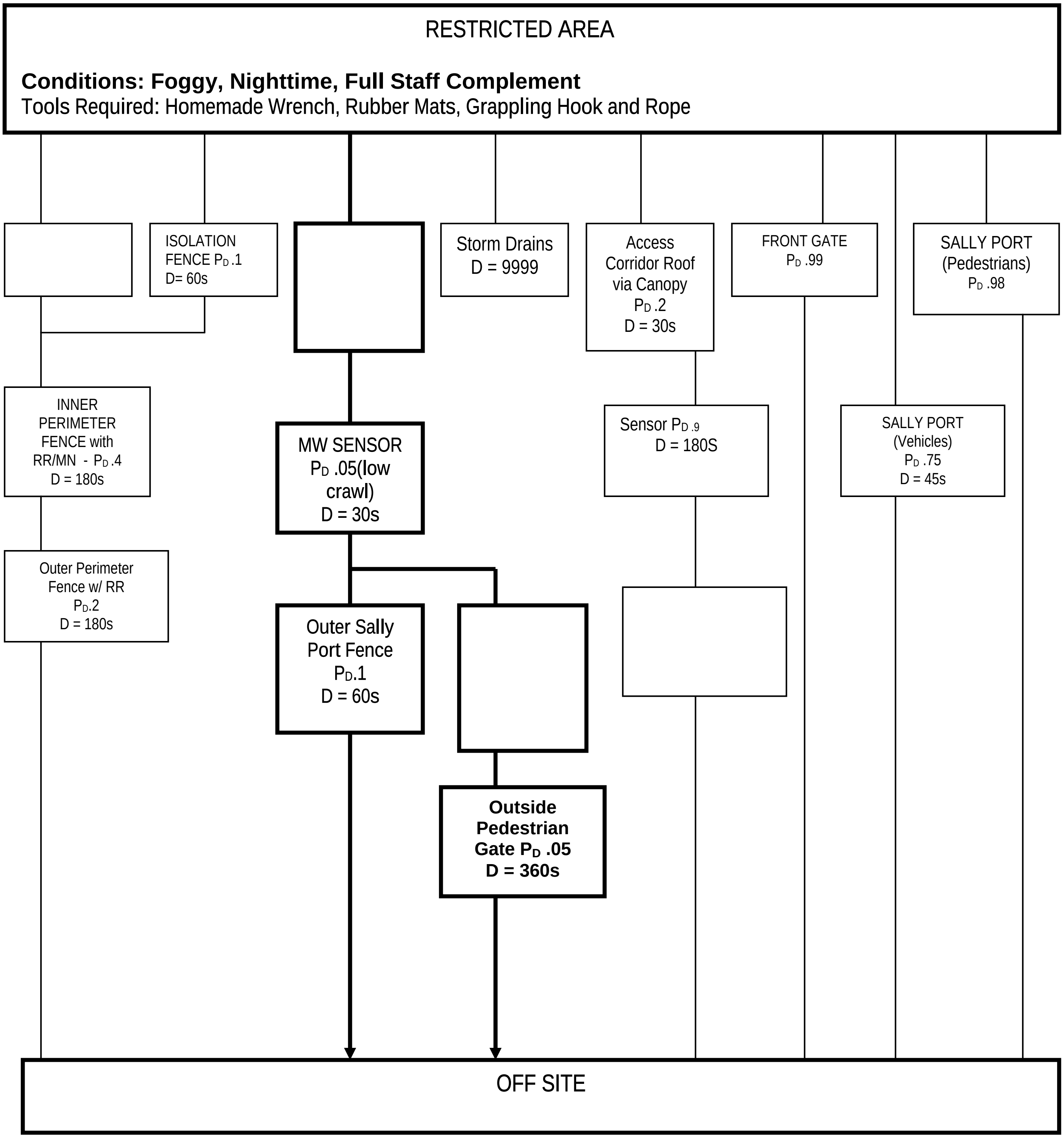
To determine the most vulnerable paths, the team used a graphical model to help evaluate the effectiveness of the PPS at the institution. These graphical models, called Path Sequence Diagrams (PSDs), were used to identify the paths to accomplish the undesired events. Each of the PPS elements along the path was defined. To identify specific scenarios and to determine the most vulnerable paths the team followed these steps:

- Annotate the PSD areas and elements with detection probabilities and delay times. **Note**: For this document, when the delay time is given as 9999, the VA Team has determined that the path is illogical.
- Look for scenarios/paths through the PSD with the lowest **detection** potential.
- Look for scenarios/paths through the PSD with the lowest **delay** time potential.
- Intuitively evaluate the paths considering response force time. While the probability of detection given for delays with electronic detection systems for some areas was considered very low, this was based upon the assessment factor. True detection does not occur without true assessment. As an example, the doors alarmed when tested 10 times; however, no staff responded to the alarm. Rating of the alarm would be a .95 probability of detection; however, as no assessment occurred. the probability of detecting an adversary (inmate) is reduced significantly. Therefore, the P_D may receive a value of .05.
- Use the EASI computer software tool to determine the probability of interruption for each event, participant, and correctional facility state.

Detailed Path Sequence Diagrams (PSDs) were mapped for the worst-case scenarios.

Path Sequence Diagram Escape Scenario 1




RESTRICTED AREA
Conditions: Foggy, Nighttime, Full Staff Complement
Tools Required: Homemade Wrench, Rubber Mats, Grappling Hook and Rope
ISOLATION FENCE PD .1 D= 60s
Storm Drains D = 9999
Access Corridor Roof via Canopy PD .2 D = 30s
FRONT GATE PD .99
SALLY PORT (Pedestrians) PD .98
INNER PERIMETER FENCE with RR/MN - PD .4 D = 180s
MW SENSOR PD .05(low crawl) D = 30s
Sensor PD .9 D = 180S
SALLY PORT (Vehicles) PD .75 D = 45s
Outer Perimeter Fence w/ RR PD.2 D = 180s
Outer Sally Port Fence PD.1 D = 60s
Outside Pedestrian Gate PD .05 D = 360s
OFF SITE

EASI Models:

Table 1 illustrates the time line and probability of detection associated with escape scenario 1. An EASI model was run using this data to illustrate this path. Table 1A shows the results of this EASI analysis.

Table 1. Escape Scenario 1 Via Rear Loading Dock to Sally Port

Task	Time (seconds)	Accumulated Time (seconds)	P_D
	5	5	.05
	5	10	.1
	240	250	.1
	240	490	.3
	30	520	.05
	120	640	.1
	360	1000	.05

Table 1A EASI Results for Scenario 1 Analysis

Estimate of Adversary Sequence Interruption	Probability of Alarm Communication			Response Force Time (in Seconds) Mean		Standard Deviation
	0.9			300		200

Description	P(Detection)		Location	Delays (in Seconds): Mean:		Standard Deviation
	0.05	OBOSP	M	5	tested	1
	0.1	OBG	M	5	EO	1
	0.1	OBG	M	240	Tested	48
	0.3	OBCRO	M	240	partial test	48
	0.05	OBOSP	M	30	Tested	6
	0.1	OBOSP	M	120	Partial tested	24
	0.05	OBOSP	M	360	Partial Tested	72
	0.45					

Based on the values associated with the escape scenario, the following equation illustrates the associated risk for this scenario:

$R = P_O * [1 – (P_I * P_N)] * C = 1 * [1 – (.45 * 1.0)] * 1.0 = .55$

Therefore, the risk to the correctional facility associated with this type of scenario is .55. Management should judge what level of risk is acceptable, but the team believed this to be a moderately high risk.

Table 1B EASI Results after Enhancements

	Probability of Alarm Communication			Response Force Time (in Seconds) Mean		Standard Deviation
Estimate of Adversary Sequence Interruption	0.9			300		200

Description	P(Detection)		Location	Delays (in Seconds): Mean:		Standard Deviation
	0.05	OBOSP	M	5	tested	1
	0.1	OBG	M	5	EO	1
	0.1	OBG	M	240	Tested	48
	0.9	OBCRO	M	999	Enhancement	0
	0.7	OBOSP	M	30	Enhancement	6
	0.9	OBOSP	M	999	Enhancement	0
	0.9	OBOSP	M	999	Enhancement	0
	.98					

Based on the values associated with this escape scenario, the following equation illustrates the associated risk for this scenario:

$R = P_O * [1 – (P_I * P_N)] * C = 1 * [1 – (.98* 1.0)] * 1.0 = .02$

As is demonstrated by this analysis the risk is reduced from .55 to .02 by the recommended enhancements.

Conclusion

This report is a collection of observations of the physical plant and established practices at SCI-_______, analysis of possible worst-case scenarios, and suggestions by the VA Team members. The intent of this report is to provide an objective analysis of the Security of Physical Protection System at the facility and its operation. The administrative staff at SCI-_______ has the responsibility for determining the value of this report, and to what extent this analysis will impact current and future initiatives.

The VA team was only able to review the PPS and the policies & procedures for a limited amount of time over a one-week period spent on-site. Indications are that the Physical Protection System, Policies & Procedures, and the _______ staff have a very effective Physical Protection System at preventing escapes during "normal" operational/weather conditions. A few anomalies were identified in the Key Observation section that need to be reviewed and addressed. However, the PPS and the procedures utilized during adverse weather conditions ________________________________

The Team determined that the facility was at _____ risk for worst-case Escape Scenario #1, _____ risk for Escape Scenario #2, and low risk for Escape Scenario #3. The Key Observations section and the Detection, Delay and Response section provide additional information about possible methods to circumvent the security systems.

Based on the team's observations and the path analysis of escape and contraband scenarios, the team concluded that the _______ area was the focus for most concerns. The majority of the worst-case escape paths and several worst-case contraband paths led through the _____, making it the weakest area in the physical protection system. If SCI _______ can focus their upgrades and enhance procedures in this area, many of these shortcomings can be addressed with minimal effort and cost.

VA Team members strongly suggest that appropriate staff within the facility evaluate the report, review recommendations, and establish short-term and long-term action plans to reduce the risk of undesirable events at the facility.

Appendix A

Detailed Vulnerability Assessment Team Observations

The information contained in this report prior to this section is considered by the VA team to be the overall primary concerns discovered during the analysis. The following information consists of observations, suggestions, and/or concerns noted by individual team members during the analysis.

A, B, C, D, E, and F Housing Units

Issue:

Issue:

G Housing Unit

I and J Housing Units

H Unit (L-5)

The L-5 housing unit has four pods with twenty-four cells per pod. All pods house Administrative Custody (A.C.) and Disciplinary Custody (D.C.) inmates, with a total of ninety-six cells. The cell doors are of steel construction with

Daily staffing.

The officers carry keys that

Each cell is searched

L-5 Exercise

L-5 Visiting

Appendix B

Threat Statement

The subject matter experts from _______ considered actual events and the generic characteristics to derive the following specific threat statement. It was divided into threats that were considered in the VA and those NOT considered in the VA.

Threat for (considered in VA)

Inmate Escape—unauthorized breach of perimeter fence from inside to outside

- Alone or with up to five other inmates
- Can use stealth, deceit, and violence (any combination)
- Tools restricted to those available inside facility (or authorized to be brought in) including ladders and rope
- Clothing and props (disguises)
- Weapons limited to improvised gun (zip) with one round of ammunition, shanks, and other material inside facility
- Inmate using a vehicle to forcibly exit the perimeter
- Staff assistance (passive—provide information only)
- Starting point may be cell
- Tunneling or use of storm/sewage plumbing

Introduction of Contraband by visitor—assist in the introduction of contraband (drugs, communication equipment, tools, and weapons)

- Non-violent

Introduction of Contraband by Staff—assist in the introduction of contraband (drugs, communication equipment, tools, and weapons)

- Non-violent

Introduction of Contraband by Inmate—assist in the introduction of contraband (drugs, communication equipment, tools, weapons, and disguises)

- Non-violent

Threat for (not considered in VA)

Inmate Escape

- Active assistance from outsider (Crash into the prison through the gate, disable RF vehicle or RF person, etc.)
- Active assistance by staff or contractor (ignore alarms, leave gate open, erroneous inmate count, etc.)
- Restricted tools or weapons introduced on site using abnormal paths (i.e., weapons or tools thrown over fence)
- Classification 2R or 2M inmates escaping from outside the perimeter (i.e., the administration building, warehouse, automotive shop, etc.)

- Classification 2M inmates escaping from outside the perimeter on community service jobs
- Inmates being transported to another location off-site. (Note: This area may need additional independent analysis. As escapes become more difficult from within, this may be the alternative of choice.)

Visitors (assist in the introduction of contraband)

- Throwing of contraband over the fence into the perimeter
- Drugs hidden in body cavities

Staff (assist in the introduction of contraband)

- Collusion with multiple staff

Inmate (assist in the introduction of contraband)

- Contraband used while outside the perimeter or swallowed to cross the perimeter boundary

Inmate Violence

- Violence toward staff, contractors, other inmates
- Riots

Inmate Suicide

Inmate suicide

A PRIMER ON PHYSICAL PROTECTION SYSTEMS (PPS)

This excerpt from the Correctional Vulnerability Assessment Handbook is reprinted with permission.

The following pages provide a primer on detection systems, in an effort to give all participants in the CVA process a common understanding of the basics. We will identify the resources needed to provide detailed evaluations of detection capabilities.

Why? So you will be able to calculate the "probability of detection" for elements of the physical protection system. Probability of detection (expressed as P_D) is one of the critical components of the EASI model that determines the overall probability of success or failure.

1. Interior and Exterior Detection Systems

This section of the handbook will provide the following:

- Introduction
- Sensor fundamentals
- Exterior sensor technologies
- Interior sensor technologies
- System considerations
- Summary

a. Introduction

Detection occurs when an event is assessed by an authorized person. The typical sequence of events is:

Alarm + Assessment = Detection

Assessment is usually-- but not always-- preceded by an alarm. For example, an officer might discover an inmate who is out of place during his/her rounds. In this instance there is no alarm, but the officer assessed the situation and determines that an unauthorized event is occurring, which means the event has been detected.

Another detection sequence might look like this:

1. Motion detector is triggered by an inmate who is in an unauthorized area. (Alarm)
2. Control center sends an officer to investigate. (Assessment)
3. Officer discovers inmate and reports it to the control center. (Detection)

A variation of the preceding might eliminate the need for the officer to investigate. The control center officer might have the ability to view the inmate using closed circuit television, allowing assessment to occur and detection to be accomplished.

There are countless detection scenarios, but all of them have the following in common: w**ithout assessment, there is no detection.**

Where does detection occur in the following set of activities?

1. Perimeter sensor alarm signal is generated
2. Alarm signal is transmitted to console
3. Operator is alerted by incoming alarm
4. Operator scans detection zone of alarming sensor for cause (either visually or with CCTV)
5. In searching for cause of alarm, operator observes an unauthorized person in that area
6. Operator notifies response force, identifying nature and location of intrusion
7. Response force interdicts intruder or escapee

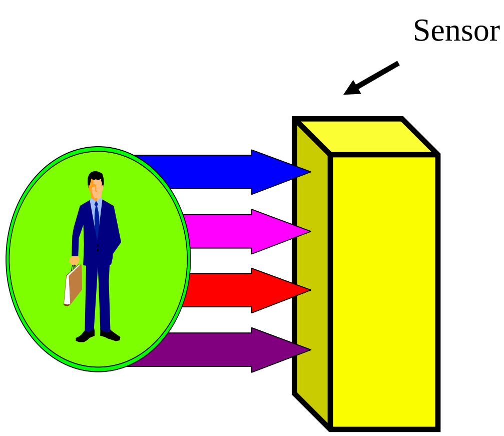
It is not until #5 (operator observes an unauthorized person) that detection occurs.

There are several physical components that are often involved with detection. These include:

- Exterior intrusion alarm
- Interior intrusion alarm
- Alarm communication and display
- Assessment
- Entry control

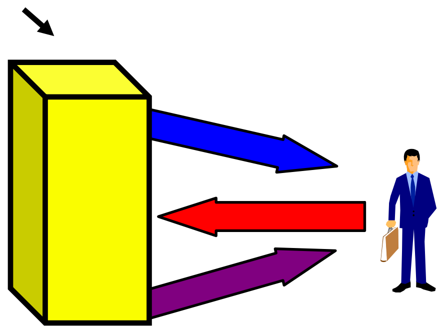
There are two types of sensors: active and passive. A passive sensor has a receiver that detects vibration, heat (infrared), sound or capacitance (electrical charge). In a passive system, the sensor receives input from the target, as shown below.

Figure III.1: Passive Sensor



An active sensor has a transmitter and a receiver. It sends a signal and detects a target by analyzing the return (see Figure III.2 below.) Active sensors include microwave, infrared, RF (radio frequency) and other technologies.

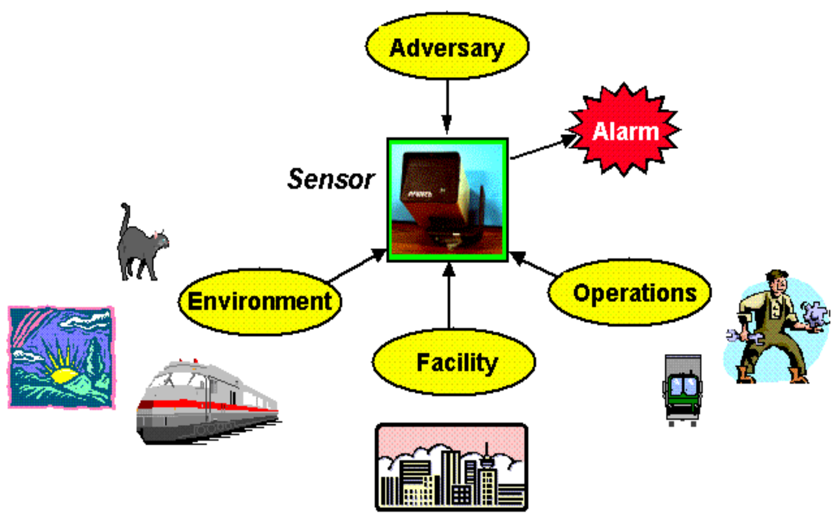
Figure III.2: Active Sensor



You may hear a sensor referred to as "bi-static." This simply means that it has a transmitter and a receiver.

Sensors are designed to interact with the setting around them. Unfortunately, you are not able to control what a sensor detects, which may lead to some difficulties. As Figure III.3 suggests, there are many targets and events that might trigger an alarm.

Figure III.3: Sensor Interactions



Several factors will determine how well a sensor performs, including:

- Sensor characteristics
- Sensor condition (maintenance)

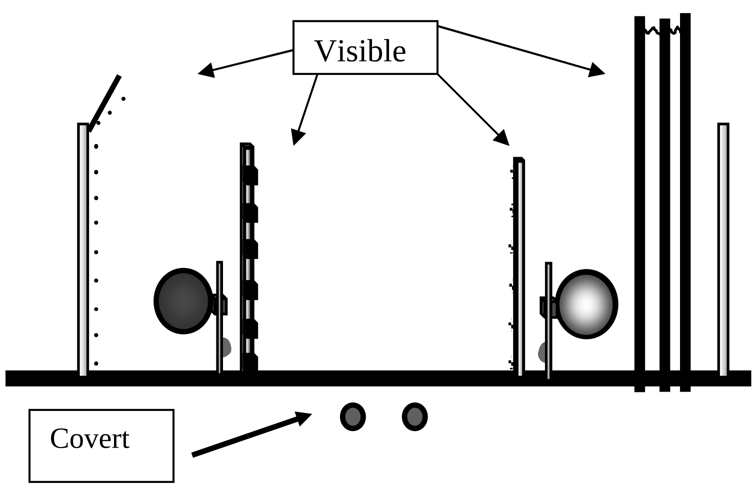
- Probability of detection (does the sensor alarm when it is supposed to?)
- Nuisance alarm rate (NAR)
- False alarm rate (FAR)
- Vulnerability to defeat

The probability of detection is also conditioned on:

- Target size and speed
- Sensor hardware
- Installation conditions
- Sensitivity setting
- Weather conditions
- Maintained condition
- Method of intrusion
  - Walking
  - Jumping
  - Tunneling

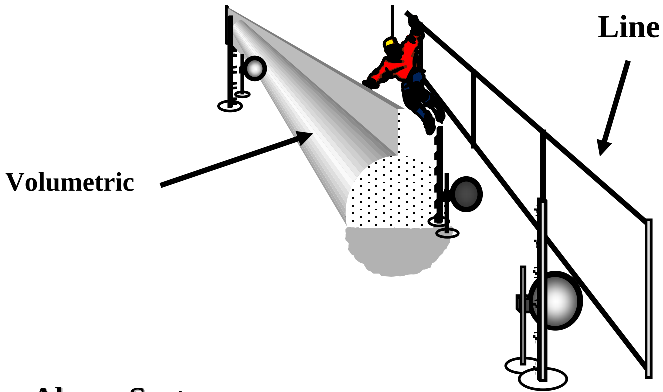
Covert systems are not easy to see, while visible systems are easily viewed. Obviously, covert sensors are more difficult for an intruder to detect. Visible systems are easier to install and maintain, though.

Figure III.4: Visible and Covert Systems



Volumetric sensors provide detection in a volume of space and their detection area is not usually visible. Line sensors provide detection along a line and the detection zone is usually easy to identify.

Figure III.5: Volumetric and Line Sensors



b. Exterior Alarm Systems

There are several types of intrusion sensor technologies:

- Microwave
- Active infrared
- Passive infrared
- Buried cable
- Vibration
- Sensor coil
- Taut Wire
- Video motion detectors
- Ultrasonic
- Sonic

Exterior microwave systems have several characteristics. They are:

- Active (send a signal)
- Visible (are readily apparent to the observer)
- Line-of-sight (must have unobstructed field of vision)
- Freestanding
- Volumetric
- Two classes of sensors
  - o Bistatic (transmitter and receiver)
  - o Monostatic (receiver only)

Exterior microwave systems have very specific site requirements. It is important to understand these requirements to ensure that systems are properly installed and maintained. The requirements include:

- ▪ Sensor bed-- The surface over which the microwave passes must be very flat-- no more than 6 inches of variation. Obstructions in the surface will create voids behind which the microwave will not be effective.
- ▪ Antenna height-- 18 to 24 inches above the sensor bed surface to the center of the cone

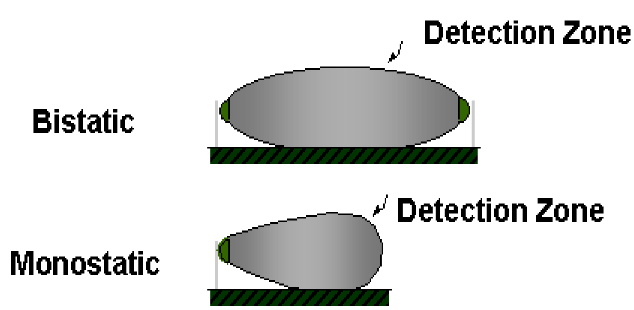
- Slope of plane- No more than a one inch elevation change in 10 feet from any point on the surface of the plane (note that this does not necessarily mean that the field has to be level, but it must be a continuous plane with little variation if it is on a slope)

Performance characteristics for exterior microwave systems vary. The probability of detection (P_d) varies with:

- Direction of movement-- the system is most sensitive to movement across the field-of-view (perpendicular to the line between of the signal)
- Velocity of the intruder (a slow crawl may sometimes defeat it)
- Height and angle of installation

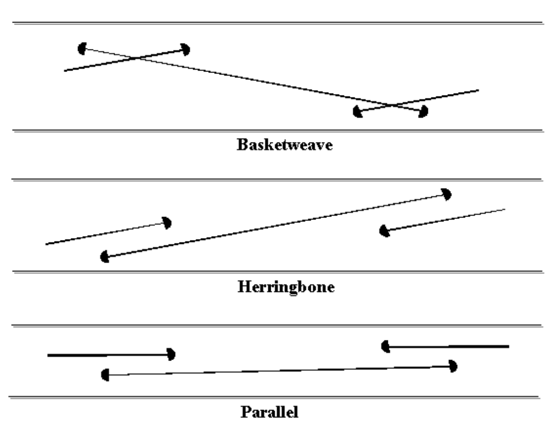
Figure III.6 shows the detection zones for the two types of microwave systems. Note that these detection zones are volumetric (e.g. shaped like a cigar, three-dimensional).

Figure III.6: Detection Zones for Microwave Systems



To respond to the detection zones, there are several types of installation patterns (see Figure III.7).

Figure III.7: Microwave Installation Patterns



Fence disturbance sensors come in many forms. They have the following characteristics in common:

- Passive
- Visible
- Terrain-following
- Normally installed on existing fence
- Line sensors
- Detect penetration or climbing of fence
- Types
  - Mechanical
  - Sensor Coil
  - Strain sensitive cable
  - Fiber optic

Some may be defeated by a very slow climb. These systems essentially turn the fence into a microphone. The system is "tuned" to alarm to specific types of input, such as the signature of a tool cutting a chain link, or a series of two or more vibrations. It is important to know the specifications of such systems, and to train persons who are testing these systems to use the right techniques.

Taut wire sensors may be freestanding or attached to the fence. These sensors are:

- Passive
- Visible
- Terrain-following
- Freestanding or attached to fence
- Line sensors
- Sensor fence section
- Types
  - Mechanical switch
  - Strain gauge / piezoelectric device

These sensors work on several operational principles: motion (often a mercury switch which is tripped by the low frequency movement of the fence; shock (detection is usually by a mechanical means); and analog (piezoelectric crystals, fence mounted geophones, electric or fiber optic cable.) Performance is affected by fabric tension, processor settings, rigidity of the fence, factors affecting noise coupling of the fence, and aids used by the intruder.

Video motion detectors (VMD) are being employed more frequently as the technology is refined and as costs decline. VMDs are:

- Passive
- Covert
- Line-of-sight / terrain-following
- Installed with other video assessment equipment

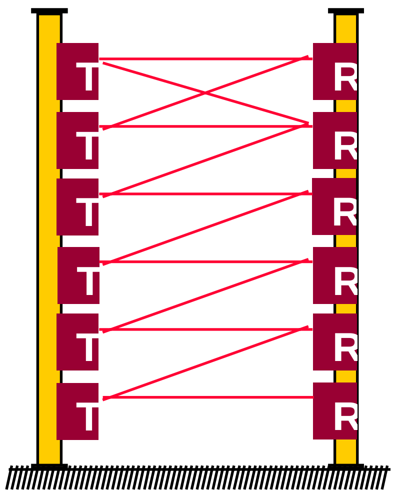
- Line sensor / volumetric

Active Infrared (AIR) systems have the following characteristics:

- Active
- Visible
- Line-of-sight
- Detection zone (basically a vertical plane)
- Single or multiple beam systems

The probability of detection for AIR systems can be very high for multiple beam sensors, but the detection zone is usually narrow, high, and is not in contact with the ground.

Figure III.8: Detection Zone for Active Infrared Sensors

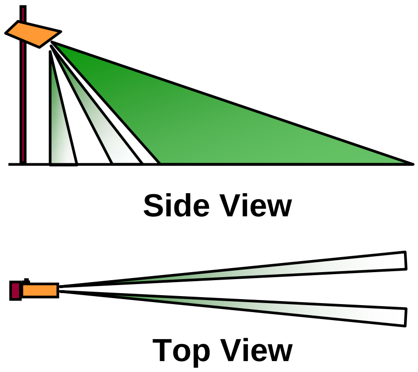


Passive Infrared (PIR) have the following characteristics:

- Passive
- Visible
- Line-of-sight
- Free-standing
- Volumetric
- Detect changes in infrared radiation within a specific field-of-view

PIR is most sensitive to movement across the field of view, and is sensitive to the velocity of the intruder (slow speed might evade detection.) The height and angle of the installation affect the probability of detection greatly.

Figure III.9: Passive Infrared (PIR) Detection Zone



Ported coaxial cable sensors are installed underground. The sensor is an electromagnetic sensor using 2-3 coaxial cables buried parallel to each other and a processor.

Ported coaxial cable sensors are:

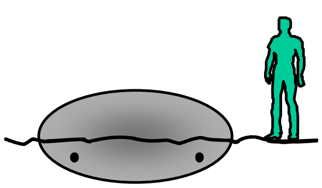
- Active
- Covert
- Terrain-following
- Volumetric
- Types
  - Pulsed
  - Continuous wave

Performance is affected by:

- Processor settings
- Orientation of intruder
- Soil characteristics (clay, sand, iron)
- Presence of metallic objects

Figure III.10 shows the detection zone for this type of sensor.

Figure III.10: Ported Coaxial Cable Detection Zone



Sandia National Labs has determined the relative probability of detection for these exterior sensor systems, as shown in Figure III.11.

Figure III.11: Relative Probability of Detection- Exterior Sensor Systems

Intruder	Electric Field	Microwave	Active Infrared	Passive Infrared	Fence Motion	Taut - Wire	Ported Coax	VMD
Walking	VH	VH	VH	VH	N/A	N/A	VH	VH
Slow Walk	VH	H	VH	H	N/A	N/A	H	H
Running	VH	H	VH	H	N/A	N/A	VH	VH
Rolling	H	M-H	M-H	M-H	N/A	N/A	VH	VH
Crawling	VH	M-H	M-H	M-H	N/A	N/A	VH	VH
Jumping	VH	M-H	H	M-H	VH	VH	H	H
Tunneling	VH	VL	VL	VL	L	VL	M	M
Trenching	L	L-M	L	L	L	VL	VH	VH
Bridging	L	L	VL	L	VL	VL	L	L
Cutting	H	N/A	N/A	N/A	M-H	H	N/A	N/A
Climbing	H	N/A	N/A	N/A	H	H	N/A	N/A

Key: VL - Very Low
L - Low
M - Medium
H - High
VH - Very High
N/A - Not Applicable

Source: Sandia National Laboratories

SNL has also estimated the susceptibility of each system to various types of nuisance alarms.

Figure III.12: Relative Susceptibility to Nuisance Alarms

Environment	Electric Field	Microwave	Active Infrared	Passive Infrared	Fence Motion	Taut - Wire	Ported Coax	VMD
Wind<47km/h	L	VL	VL	VL	L	VL	VL	L-M
Wind 47-115km/h	M	L	L	L	H	VL	VL	L-M
Wind>115km/h	M	L-M	L-M	L-M	VH	L	VL	M
Rain	L-H	L	L	L-M	M	VL	M	L
Snow	M	L-M	M	L-M	L	VL	L	M
Fog	VL	L	M	L	VL	VL	VL	L-M
Small Animals (Rabbits)	M	M-H	M	M-H	VL	VL	VL	M
Large Animals (Dogs)	VH	VH	VH	VH	L	L	M	M-H
Small Birds	L	VL	L	L	L	VL	VL	M-H
Large Birds	M	M	M	M	L	VL	VL	M
Lightning	M	L-M	L	L	L	VL	M	L-M

Key: VL - Very Low
L - Low
M - Medium
H - High
VH - Very High
N/A - Not Applicable

c. Interior Alarm Systems

There are even more sensor technologies available for interior applications than there are for exterior use. Interior systems include:

- Balanced magnetic switches
- Glass break
- Photoelectric
- Microwave
- Ultrasonic
- Passive infrared
- Video motion detection
- Capacitive
- Fiber optics
- Vibration

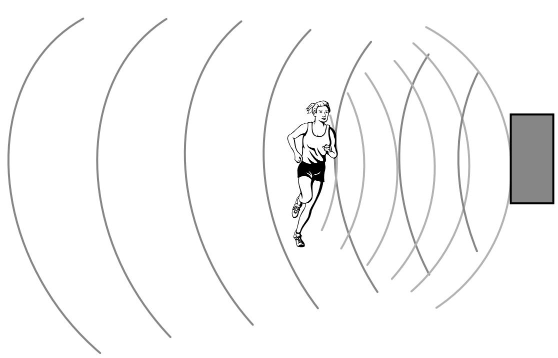
Boundary penetration sensors include magnetic switches (such as a door position indicator), glass break sensors, and photoelectric sensors. Photoelectric sensors provide line of sight protection and have a relatively long range. They are active systems that have low false alarm rates (FAR). The major types of glass break sensors are shock, frequency, shock/stress, and passive audio.

Interior motion sensors have a broader range of detection than boundary penetration sensors because motion sensors have volumetric detection zones. There are several types of interior motion sensors:

- Microwave
- Ultrasonic
- Video motion
- Sonic
- Infrared

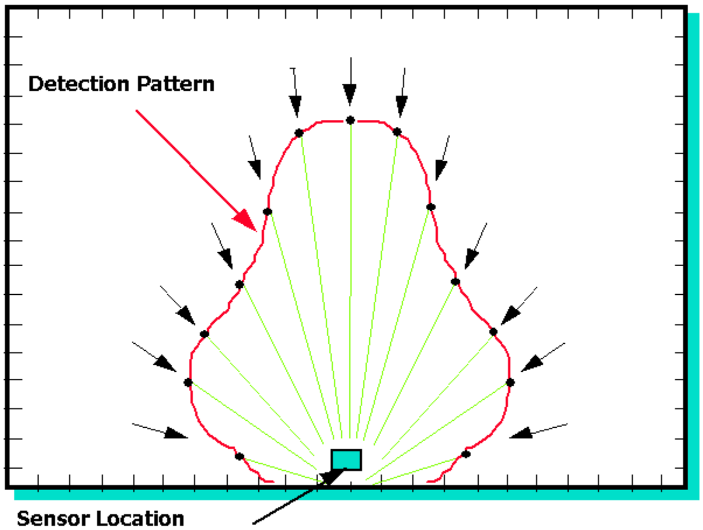
Microwave sensors transmit energy and monitor the return through a receiver. The motion of an intruder alters the pattern and frequency of the "return" and causes a shift in the frequency. If there is sufficient amplitude change and duration time, an alarm is sounded.

Figure III.13: Microwave Sensor



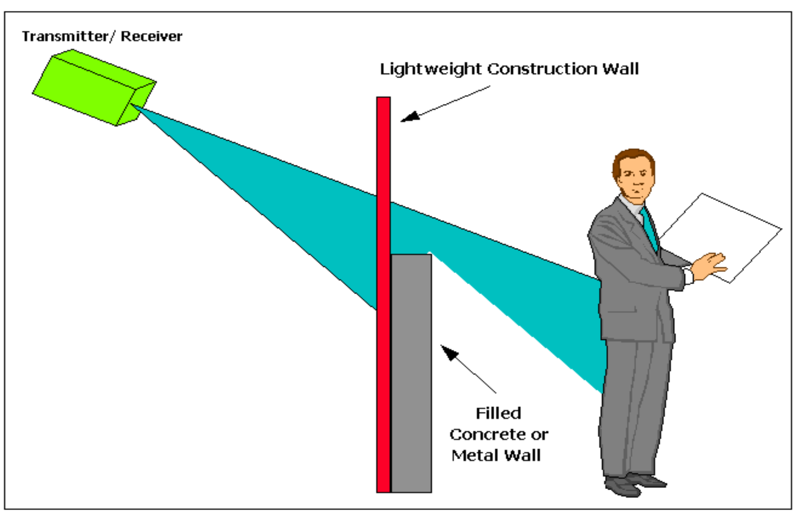
The detection pattern for a microwave sensor is shown in Figure III.14, which demonstrates for doppler effect.[1] The effectiveness of detection will vary with the direction an intruder is moving. For example, if an intruder is moving left to right on the diagram below, detection will be higher than if the intruder is moving in a line toward the sensor. And as with exterior microwave applications, time and mass trigger the alarm and a low fast crawl may sometimes defeat it.

Figure III.14: Microwave (Monostatic) Doppler Detection Pattern



A word of caution about monostatic microwave sensors: microwaves will *penetrate* walls and other barriers that are of light construction. This may result in false alarms when there is movement in an adjacent space. Figure III.15 depicts this characteristic.

Figure III.15: Monostatic Microwave Penetration

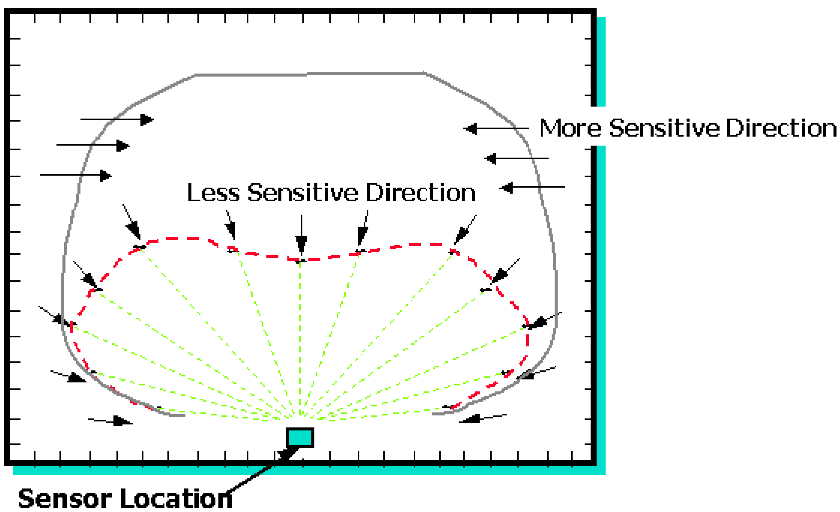


[1] The "doppler effect" means that the frequency and wavelength of an electromagnetic field is affected by relative motion.

Ultrasonic motion sensors are used in an active system that also provides true volumetric protection. The surveillance area for ultrasonic systems is defined by the walls, floor, ceiling and windows.

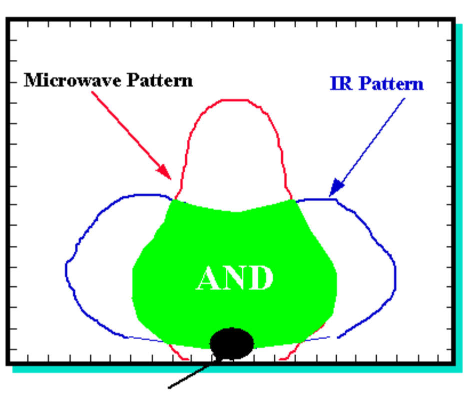
Passive infrared (PIR) detects by receiving infrared energy from objects. Ceilings, walls, floors, furniture and other objects emit infrared energy that is proportionate to their temperature. Motion is detected by measuring changes in the received infrared energy. Figure III.16 provides an example of the PIR detection pattern. As with the microwave sensors, detection is more sensitive for intruders moving across the detection area (left and right on the diagram below), while the least sensitive direction would be a path moving straight toward the sensor.

Figure III.16: Sample Passive Infrared (PIR) Detection Pattern (walking at 1 foot per second)



Combination sensors systems usually employ microwave *and* infrared. These systems allow for a higher sensitivity setting and reduce the incidence of false alarms (FAR). But the probability of detection is lower for these systems because the intrusion must be detected *twice*-- once by each type of sensor. Figure III.17 shows the detection pattern for a typical combination sensor system.

Figure III.17: Combination Sensor System Detection Pattern



So many choices...which is "right?"

There are no absolute right or wrong answers when considering detection systems. The goal is to find the system that works best for each unique application. It is also important to understand what each system can, and *cannot* do. Figure III.18 provides a comparison of the features of the various systems.

Another consideration in selection of the right system(s) is the consequence of component failure. A system that becomes inoperable when one component fails is less reliable than one that has redundant systems or equipment that can take over when a component fails. In some systems, aid from sources outside the institution is required to restore the component to a functioning condition.

Figure III.18: Interior Sensor Selection

Applications	Operating Principle	Detection: Portal Opening	Detection: Breaking Through Wall, Floor, Ceiling	Detection: Radial Motion	Detection: Transverse Motion	Detection: Touching Object	Conditions for Unreliable Detection	Typical Defeat Methods	Major Causes of Nuisance Alarms: Air, Humidity, Temperature	Localized Heating	Movement Outside Area	Fluorescent Lights	Loose Fitting Doors	Mount Vibration	Ambient Acoustic Noise	Rodents, Animals	Radio Freq Interference
Boundary Penetration	Balance Magnetic	+					Improper Installation	Stay-Behind Intruder or Entry Through Unprotected Area					−				
	Vibration		+								−			−			
	Intrasonic	+	+						−				−				
Interior Motion	Sonic	+		+	+				−					−	−	−	
	Ultrasonic	+		+			Air Movement	Cover When Sensor is in Access Mode	−					−	−	−	
	Microwave	+		+			RFI				−	−		−		−	−
	Infrared				+		Variable Thermal Background			−				−		−	−
Proximity	Capacitance					+	Given Changes in Humidity, Temperature, or Pressure	Disable Electronics	−							−	
	Pressure Mat					+										−	

Source: Sandia National Laboratories

A good system for your application would have the following characteristics:

- *High* probability of detection (P_D)
- *Low* nuisance alarm rate (NAR)
- *Low* vulnerability
- *Fast* communication system
- *Good* lighting/assessment system
- *Balance* - a system approach
- *No* single point/component failure
- *Good* protection in depth

A *balanced* physical protection system provides adequate protection along *all* possible paths. Failing to consider all paths is like installing a highly secure lock on the front door of your house, but leaving the back door open.

The realities of institutional operations require that a balance is achieved between:

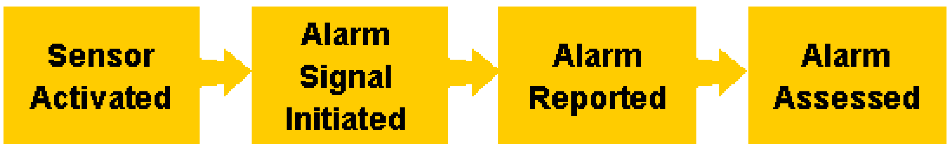
- Cost
- Safety
- Structural integrity

The EASI tool, introduced in Section II of this handbook, provides an excellent resource for modeling the impact of enhancements and improvements in your physical protection systems. EASI will help you to determine which approaches and systems reduce risk the most. Unfortunately, many of the upgrades provided for our institutions are prompted by tragedy and are funded in an effort to throw money at the problem rather than consider the complete picture. The EASI tool provides a more rational approach to system improvements.

2. Alarm Communication and Display

The preceding pages addressed methods and sensor systems that may be employed to detect intruders or other undesired events. For true “detection” to occur, each of the following steps must be complete.

Figure III.19: Elements of Detection



Several performance measures may be applied to the detection process, including:

- Probability of detection
- Time for communication and assessment
- Frequency of nuisance alarms

- Frequency of false alarms

Remember, alarm without assessment is not *detection*.

A sensor is useless if it is not able to communicate an alarm to the appropriate person or people. Figure III.20 presents a diagram of a typical traditional annunciator panel system, identifying the function of each component.

Figure III.20: Traditional Annunciator Panel System

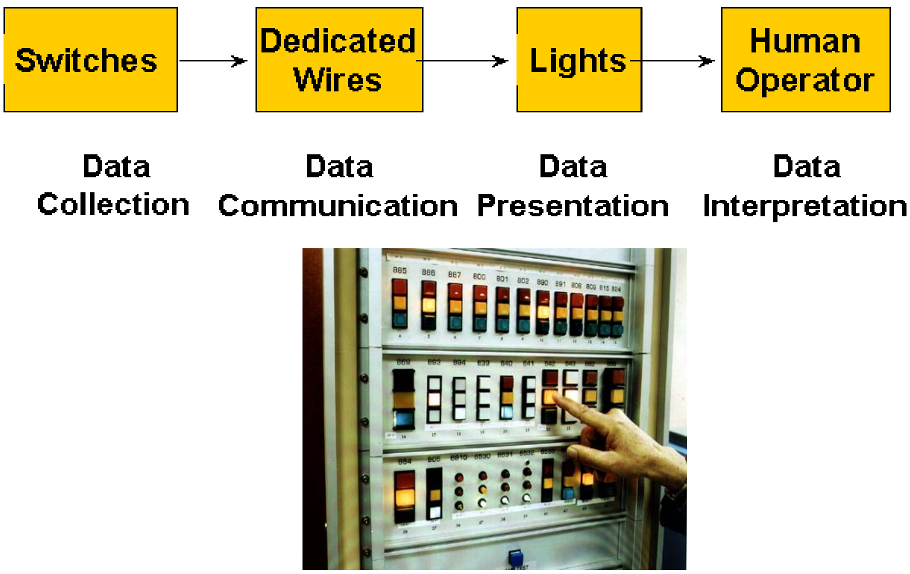


Figure III.21 shows the more modern integrated system.

Figure III.21: Integrated Display and Assessment Systems

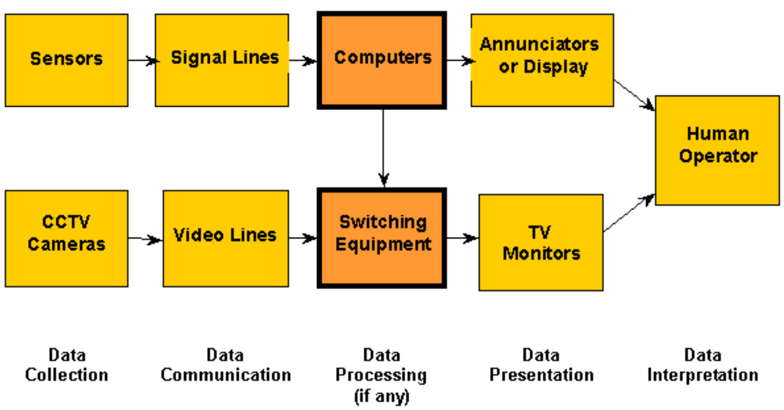


Figure III.22 provides a whimsical portrayal of what *not* to do. In this situation, which is often encountered in correctional facilities, the operator often turns off some of the alarms.

Figure III.22: Alarm Overload

What are the characteristics of a good alarm communication system? The preferred features include:

- Fast reporting time
- Supervision of all cables (cables not easily tampered with)
- Easy and quick discovery of single-point failure – redundancy
- Isolation and control of sensor
- Expansion flexibility

Common sense tells us that cables should be not be placed on the "threat side" of a sensor, where an intruder may have easy access to it. Similarly, alarms should be triggered if a cable or other communicating element, such as a cable, is disabled. Of course, redundancy is important whenever it is feasible.

There are many options available, and the choices are expanding as technology evolves. It is important to understand the unique characteristics of your site and installation.

<u>Video systems</u> are found in almost every institution, although there are many variations in their application and technology. The major components of a video system are:

- Camera, lens and mount
- Lighting system
- Transmission system
- Video switching equipment
- Video recorder (often digital now)
- Video monitor
- Video controller

A video system has many potential uses, including:

- Confirming that an electronic alarm is real
- Providing identification of what caused the alarm
- Providing general surveillance of an area
- Identifying people in the area
- Identifying unusual activity of any kind in the area

Consoles also vary, but usually display the following information:

- Zone status (secure, access, alarm)
- Assessment information
- Procedural instructions
- System status
- Alarm history

Information may be displayed as text, graphics, or as a combination. Many new systems use touch screens or a computer mouse.

Typical operator functions include:

- Start and end assessment of alarms
- Set individual sensors into access or secure
- Open and close doors/buildings
- Display system status
- Request procedural instructions
- Assign CCTV cameras to video monitors
- Start and stop recording
- Examine system log

As with sensors, *redundancy* is important. This might involve backup equipment and procedures or duplicate consoles. Emergency power supply and an uninterruptible power supply for computers are essential.

3. Entry Control and Contraband Detection

The following text and diagrams provides an overview of entry *and exit* control and contraband detection systems, explores various types of badges, and examines the characteristics of contraband detectors.

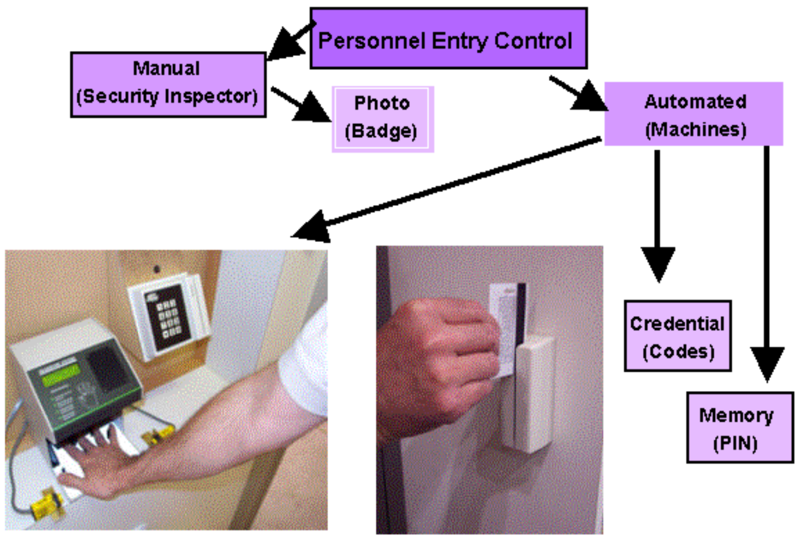
The purpose of entry control is to:

To allow entry of: authorized people
authorized material

To allow exit of:	authorized people authorized material
To prevent entry of:	unauthorized people weapons and other contraband
To prevent exit of:	unauthorized people

Figure III.23 shows the various types of entry control systems.

Figure III.23: Entry Control Systems



Several types of badge technologies may be found in correctional institutions, including:

- Photo identification badge
- Bar code technology
- Magnetic stripe technology
- Wiegand technology[2]
- Proximity card technology
- Smart card technology

Any badge system is concerned with the ability to counterfeit. Figure III.24 describes the ease of counterfeiting for several types of coded badges.

[2] Wiegand technology is a proprietary card system that is very difficult to duplicate

Figure III.24: Ease of Counterfeiting Coded Badges

- Proximity read ↓ difficult
- Direct read
  - Magnetic stripe ↓ easy to difficult
  - Bar code ↓ easy
  - Wiegand wire ↓ average
  - Smart card ↓ difficult

Similarly, the probability of detection for counterfeit badges has been calculated by Sandia National Laboratories.

Figure III.25: Relative Probability of Detection of Counterfeits

H

- Biometrics and PIN
- Exchange picture badge and PIN
- Exchange picture badge
- Picture badge and PIN
- Picture badge
- Credential and PIN
- Credential
- Casual recognition

L

Biometric systems include hand, thumbprint, facial, retinal and iris scan technologies. A PIN is a personal identification number that is assigned to an individual. In a Texas institution, persons wishing to enter the facility are required to pass their identification and credentials into a control center to be examined by a staff member. One institution in Ohio has a video camera system that projects an image of each ID badge onto a 13-inch monitor, making it easier to identify counterfeits. All too often, the persons responsible for checking identification are so busy that they give only a cursory glance, or sometimes do not even look at all.

There is often a temptation for personnel to move fast. When lines get long and visitors and personnel become impatient, it is only natural to try to speed up the identification process. While speed was an ally when it came to communicating alarms, it is an adversary to proper entry and exit security practices. Personnel must know that they have permission, or better yet are *expected,* to take the necessary time to ensure the proper identification of every person who enters and exits the institution. Good security is not necessarily *convenient*.

Contraband detection systems fall into three major categories:

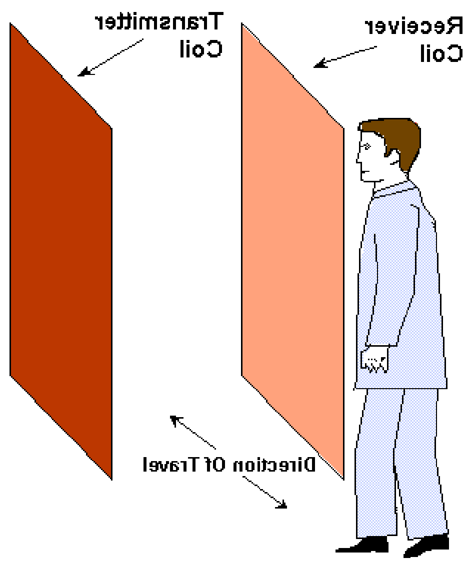
- Metal detectors

- X-ray techniques
- Emerging “sniffer” technologies

Selecting contraband detection systems, and specific devices, requires consideration of their corresponding principles of operation, sensitivity factors, and placement considerations.

Metal detectors have a transmitter coil and a receiver coil, as shown in Figure III.26.

Figure III.26: Coil Geometry for Typical Pulsed Field Metal Detector



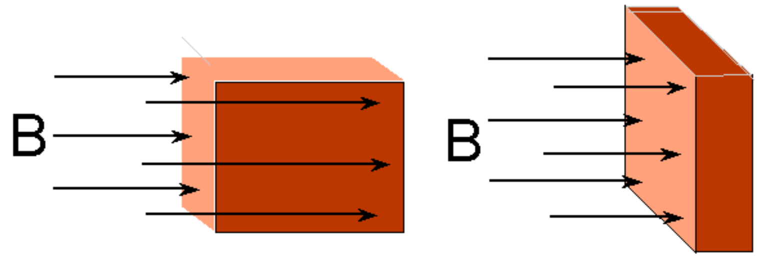
Many factors have an influence on the effectiveness of metal detectors.

- **Detector itself** (how it is programmed, its settings)
- **Objects** (weapons, personal possessions)
- **Object characteristics** (size and shape, orientation to coil, type of metal)
- **Subject walking through** (velocity, location of object on the person)
- **Environment/setting** (nearby metal, electromagnetic background such as flourescent lights, floor buffer)

Metal detectors are often defeated, deliberately and accidentally. Unfortunately, inmates often watch as the detectors are defeated. It is important that personnel who operate metal detectors are thoroughly trained and are closely supervised.

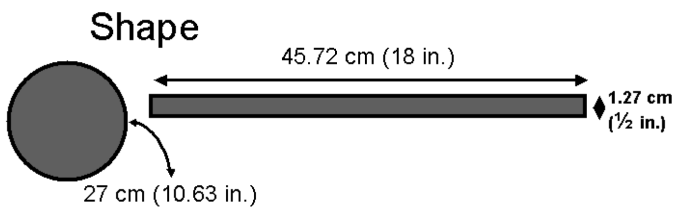
It may help to think of the metal detector as a series of arrows that go from the transmitter coil to the receiver coil. The amount of *area* that is presented to the detector will influence how well the object is detected. In Figure III.27 shows six imaginary “arrows” that represent the direction of the field in a metal detector. When the box on the left is passed through the field only three of the arrows “hit” it because it is turned sideways. But all six arrows hit the box when it is turned to face the field, as shown on the right.

Figure III.27: Importance of Orientation of Object



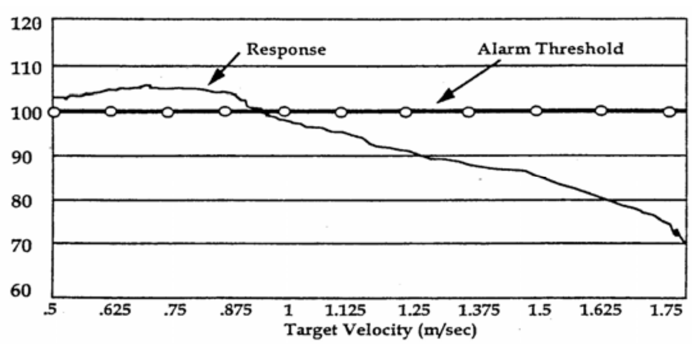
Similarly, the *shape* of an object will have a significant effect on the probability of detection. Figure III.28 shows two objects that have equal areas. But the circle is three-times easier to detect because of the shape it presents to the detector.

Figure III.28: Effect of Shape on Detection



Finally, the *velocity* at which an object passes through metal detector will also affect the probability that it is detected. Figure III.29 shows the relationship between the speed at which an object passes through a detector and its ability to be detected. The graph shows that once an object is traveling at about 1 meter per second or more, it is unlikely that it will be detected. Some persons will try to defeat a metal detector by taking a "big step" into it and moving through quickly. In response to these attempts to evade detection, some institutions require subjects to turn around while in the detector.

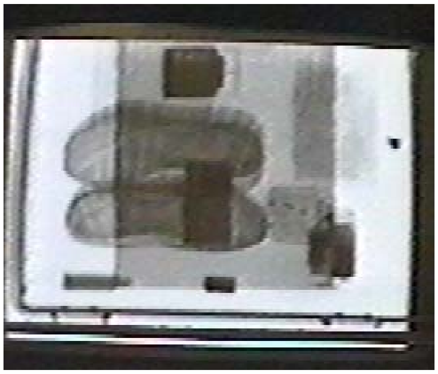
Figure III.29: Velocity of Object vs. Detection



The location of the object on the person will also affect the chances it will be detected. Metal detectors may be adjusted to focus more on certain areas. It is not unusual to find that little detection occurs in the lower area of the field. Smugglers have been known to tape metal tins with drugs to their ankles in an effort to evade detection. Similarly, weapons such as small guns or knives are often less detectible if carried very low.

X-Ray machines provide another resource for contraband detection. X-rays may be used to detect other objects, in addition to metal. For example, the two images in Figure III.30 are of the same bag. The one of the right uses backscatter technology, and it identifies explosives in the
back as light colored areas on the screen.

Figure III.30: Backscatter X-Ray Image

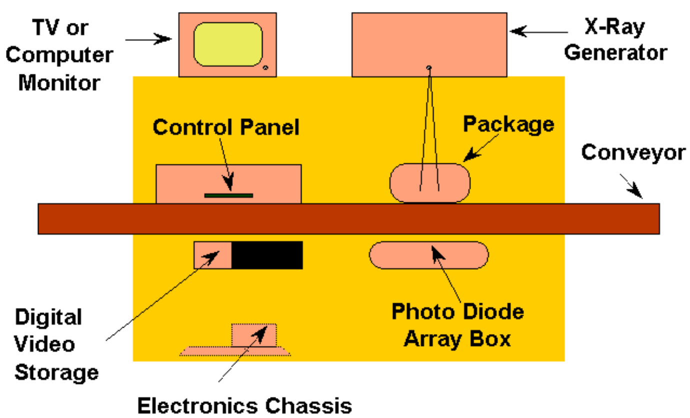


Regular X-ray

Backscatter X-ray image

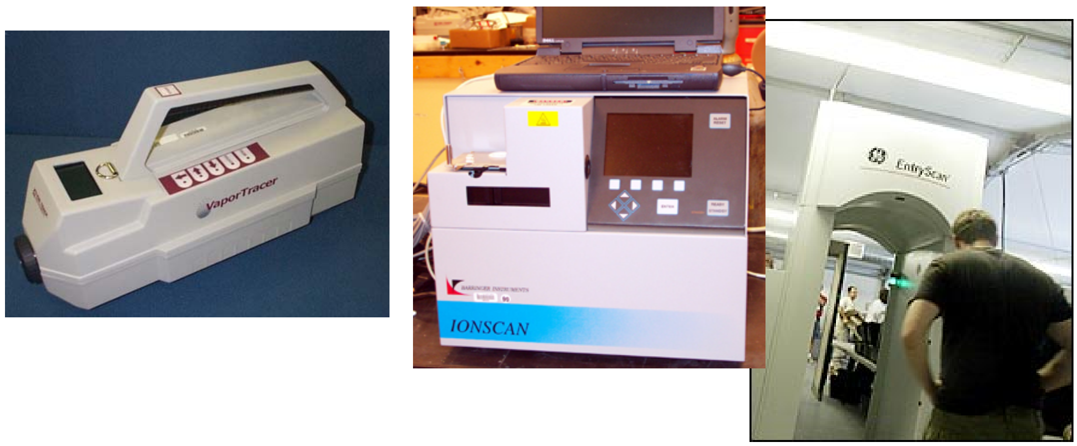
A typical X-ray package search system is shown in Figure III.31. X-ray machines are capable of imaging a 26-gauge wire hidden in a test wedge, when properly operated. Personnel who operate this equipment must be well-trained and should have short duty periods to prevent loss of detection efficiency due to fatigue.

Figure III.31: Typical X-Ray Package Search System



Sniffer detectors represent a fast-evolving technology that is appearing in airports and other locations. Hand-held sniffers were initially developed for field applications. A bench model version may often be seen in airports, where personnel use a pad to wipe down surfaces of a traveler's baggage and then insert the pad for analysis. Several airports now have sniffer "portals" that look somewhat like telephone booths. The subject steps into the portal and the doors close. The portal employs a "preconcentrator" that works by drawing in a large volume of air, collecting heavy organic compounds from the air stream onto a filter, then vaporizing these organics into a smaller parcel of air that is delivered to a commercial explosives or drug detector. Figure III.32 shows the three types of sniffers.

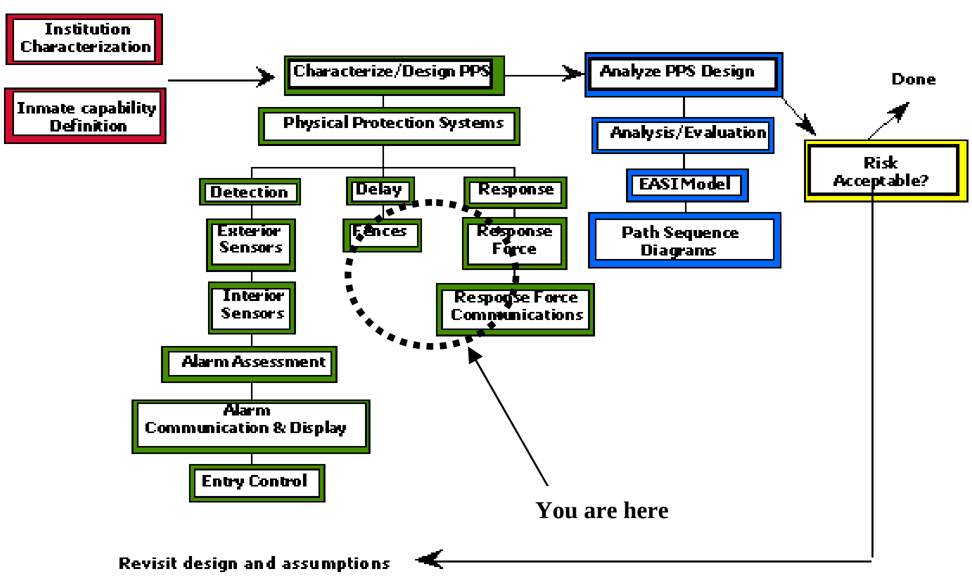
Figure III.32: Three Types of Detectors Using "Sniffer" Technology



4. Delay

Having examined detection methods and technologies in some detail, it is time to turn to the next two elements of physical protections systems (PPS). Figure III.33 shows the overall risk evaluation process and highlights our current position.

Figure III.33: Risk Evaluation Process



The checklists in Appendix D help to identify the delay features in your institution. These include, but are not limited to:

- Fences and gates surrounding the facility
- Vehicle barriers
- Construction of walls/windows/doors/roofs/floors
- Areas where detection is not provided before delay
- Areas where there are multiple layers of delay exist, i.e. locks, windows, walls, distance, fences, and razor wire

Sandia National Laboratories has tested a variety of delay and detection systems. Their findings are integrated into the EASI program spreadsheets, as a "lookup" function. Figure III.34 provides sample of their findings.

Figure III.34: Sample of Data Collected for Physical Protection System Components.

General Task	P_D and Delay Time
Climb 14 ft. fence	20 second delay (climbing)
Running with equipment	10 feet per second
Cut 1 ¾" carbon steel bar with hacksaw	30 seconds per bar
Cut hardened bars with hacksaw	60 minutes per bar
Penetrate cell door without tools	Infinite
Penetrate Metal core door	12 second delay per door
Microwave exterior detection system	0.9 probability of detection
Tilt / vibration fence sensor	0.8 probability of detection
Detectors on building doors	0.99 probability of detection
Interior detector	0.9 probability of detection
Standard deviation on all times	30% of mean

APPENDIX N: Powerpoints for
4-Day Training Program

AMERICAN JAIL ASSOCIATION

Calculating
Jail Vulnerability

Madison County
Huntsville, Alabama
May 2008

Sponsored by:

Madison County Sheriff's Office

Today's Agenda

- **Introductions**
- **JVA Overview**
- **Threat Definition**
- **Threat Capabilities**
- **Prep for site and location exercise**
- **Lunch, to jail**
- **Location and Site**
- **Facility layout**
- **Identify target areas for Day Two**

The Rest of the Week

All days on site at the facility

<u>Tuesday</u>: Identify observations and analysis in five target areas through the facility

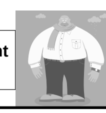
<u>Wednesday:</u>
- **Assemble initial findings and identify root causes**
- **Begin scenarios and data collection**

<u>Thursday</u>
- **Finish scenarios, analyze with EASI**
- **Present findings**
- **Assemble all findings, develop implementation plans**

Brought to you by….

- Sandia National Laboratories
- U.S. Dept. of Defense (Nuclear Weapons)
- U.S. Dept. of Energy (Atomic Asset Protection)
- National Institute of Justice (NIJ)- Adapting the tools for use in prisons
- **National Institute of Corrections (NIC)- Developing tools for use in jails**

Hi! I'm from the federal government and I'm here to help.



Handouts and Resources

- You have a copy of the ***CVA*** Handbook and appendices developed by NIJ for use in prisons
- We will be using components of these materials during this training event
- EASI, these powerpoints, and the broader CVA materials will be available to you after the training is completed

Ground Rules

- Be careful– take no risks
- Be discreet- inmates *and others* are watching and listening
- Be especially alert after the VA training
- Take notes
- Take photos, *no identifiable inmates*
- Think like our adversary
- Remember we are in an OCCUPIED and OPERATING facility
- Report serious security breeches to appropriate staff member immediately
- Respect facility staff

Experts?

- Everyone brings expertise to the table
- This works best when rank is left at the door
- Safety and security requires everyone working together, and working consistently
- Links of a chain

Take Good Notes

- Good things that you see (strengths)
- Weaknesses that you observe
- Questions that need to be answered in order to determine risk and vulnerability
- **Nothing is too small… remember the chain**

Use your composition book

Trends?

- Inmates
- Facilities
- Technology
- Staffing
- Funding
- Other

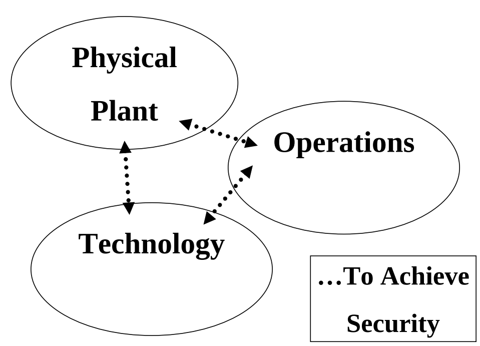
Constitutional Perspective

- **Duty to protect** from a "risk of serious harm" (inmates, employees, visitors, volunteers, contractors, etc)
- You may be found to have been "deliberately indifferent" if you failed to act within the scope of your authority to a known risk, or a risk about which you **should have known**.
- Vulnerability assessment findings are subject to discovery in civil litigation.

<u>Security Principles</u> : Maintaining security is a *continuous* process, demanding sufficient staff who are:

- ❑ qualified,
- ❑ properly trained,
- ❑ directed by policies and procedures, and
- ❑ supervised
- ❑ properly deployed (at the right place, at the right time)

It Takes All Three….

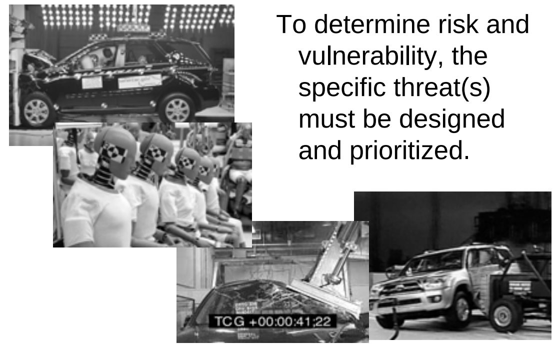


Jail Safety and Security/ Vulnerability Assessment

PROCESS

A. Threat Definition and Capability		
↓		
B. Identify Deficiencies (combine characterizing and analyzing into a series of excursions into the facility)		
↓		
C. Assemble Deficiencies and Classify		
↓		
D. Identify Root Causes	➤	1. ASDs, PSDs Scenarios
↓		
E. Create Solutions	◄	2. EASI
↓		
F. Implement		
↓ ↓		
Initial solutions	Ongoing System	

A. Threat Definition



To determine risk and vulnerability, the specific threat(s) must be designed and prioritized.

A. Threat Capability

- For each threat, understanding capabilities is necessary to measure vulnerability
- Capabilities evolve
- Capabilities will have different implications for varied threats

B. Identifying Deficiencies

- Examining the jail setting from many perspectives to identify concerns
- Using new tools to discover more risks and vulnerability

C. Assemble Deficiencies and Classify

D. Identifying Root Causes

1 and 2: Analytical Tools

1. Preparing Scenarios

- Area diagrams
- Path Sequence Diagrams
- Scenarios
- Data Collection

Advanced.. Continued

2. Using EASI to Calculate Risk

- Enter data into program
- Calculate probability of interruption
- Explore potential solutions and test them using EASI

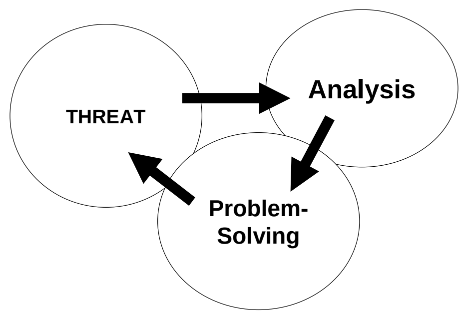
E. Creating Solutions

- Assemble all findings and corresponding root causes
- Assigning priorities
- Developing solutions, and “solution sets” to address problems

F. Implementation

- <u>Initial Actions</u>– addressing many identified deficiencies immediately
- <u>Ongoing *System*</u> to continuously improve safety and security

Continuous Safety and Security Improvement Process



Remember

Security is not convenient!

A. Threat

- Defining and assigning priorities to threats
- Identifying the “capabilities” of participants in the threat scenarios

Let's Hear About Your Facilities and Operations

- Describe your overall **<u>jail setting</u>** (size, age, design, operations)
- Identify **<u>problems</u>** and challenges you face

A: Defining the Threat

A SHOPPING LIST FOR STARTERS—

- ❑ Escape by one or more prisoners **(this is what is used in the CVA Handbook)**
- ❑ Unauthorized entry into the facility or movement within the facility
- ❑ Introduction of contraband into the facility
- ❑ Prisoner assault on staff
- ❑ Prisoner assault on another prisoner
- ❑ Major disturbance or riot
- ❑ Prisoner suicide or attempt
- ❑ External attack on the facility
- ❑ Terrorism

Participants to consider

PEOPLE

❑1. Inmates
❑2. Administrative Staff
❑3. Correctional Officers
❑4. Contractors/Vendors
❑5. Visitors
❑6. and….

27

Consider…

Important Information

1. Inmate Records
2. Personnel Records
3. Security Related Documentation, i.e. officer shift changes, assignments
4. Intelligence Information
5. Activity Schedules

And….

Consider…

Vital Equipment

1. Heavy Equipment within the Facility
2. Communication Rooms
3. Security Equipment, i.e. video cameras, sensors, and transmission mediums
4. Backup Power Source
5. Weapons/Tools

And…..

Consider…

Contraband

1. Drugs both legal and illegal
2. Money
3. Alcohol
4. Tools
5. Weapons
6. Electronic Devices

Outcome Measures (for ideas)

- ❑ physical injuries
- ❑ vehicle accidents
- ❑ emergencies
- ❑ times that normal facility operations were suspended due to emergencies
- ❑ injuries requiring medical attention that result from emergencies
- ❑ incidents involving toxic or caustic materials
- ❑ Other incidents
- ❑ unauthorized inmate absences from the facility
- ❑ instances of unauthorized access to the facility

More outcome measures…

- ❑ instances in which force was used
- ❑ weapons found in the facility
- ❑ controlled substances found in the facility
- ❑ incidents involving keys
- ❑ incidents involving tools
- ❑ incidents involving culinary equipment
- ❑ incidents involving medical equipment and sharps
- ❑ incidents in which staff were found to have acted in violation of facility policy
- ❑ staff substance abuse tests failed

Prioritizing Threats

- Can we reach of consensus on three threats that are of most concern to the group?

A. Threat Capability Definition

- ❑ ***Using all information sources determine:***
  - ❑ **Range of tactics**
    - ❑ **Stealth**
    - ❑ **Force**
    - ❑ **Deceit**
  - ❑ **Capabilities of inmates**
    - ❑ **Knowledge**
    - ❑ **Motivation**
    - ❑ **Skills**
    - ❑ **Weapons and tools**

For example, examine Facility Escape History

- ❑ Identify any past incidents and describe the details of the scenario presented by the inmate(s).
- ❑ Details should include a description of inmate tactics, weapons, escape path elements, tools used, transportation, the time of day, and weather.
- ❑ Was the inmate(s) acting in collusion with anyone from the outside and/or staff?
- ❑ Escape attempts can be accomplished by using either one or all of the following methods, deceit, force, and stealth-- identify which was used.
- ❑ Determine historical data, i.e. past/present/future, using past records and intelligence information.

Examine Contraband History

1. **Determine the type of contraband that is being brought into the facility, i.e. weapons, drugs, money, electronic devices.**
2. **Identify the means in which the contraband is being introduced into the facility, i.e. visitor areas, daily deliveries, and staff.**
3. **Determine the means in which the contraband is being packaged.**
4. **Determine the ownership of the contraband and if it is associated with a specific group or activity.**
5. **Determine historical data, i.e. past/present/future, using past records and intelligence information**.

Threat *Capabilities*

- ❑ Use past history as a starting point
- ❑ Consider:
  - ❑ **type of inmate**
  - ❑ **assistance (and type)**
  - ❑ **weapons**
  - ❑ **tools**
  - ❑ **vehicles**
  - ❑ **visitors**
  - ❑ **staff**
  - ❑ **other inmates**
  - ❑ **violence.**

Tactics

- ❑ Stealth
- ❑ Force
- ❑ Deceit
- ❑ Collusion (?)

Do Not Discount Inmate Capabilities Such As:

- ❑ Knowledge
- ❑ Motivation
- ❑ Skills
- ❑ Abilities

EXERCISE: Capabilities

- Divide into three groups
- Each group is assigned one of the priority threats
- Brainstorm the capabilities that would be associated with your assigned threat
- Record on flipchart and be ready to present

Threat Summary

- What do the three threats have in common?
- What are unique to some threats?
- Any surprises?

Step B. Identifying Deficiencies

- Examining the jail setting from many perspectives to identify concerns
- Using new tools to discover more risks and vulnerability

PHYSICAL CHARACTERISTICS

See Appendix B Checklists:

B1: Location
B2: Site
B3: Facility Design, Layout and Construction
B4: Video Systems
B5: Alarm and Sensor Systems
B6: Metal and Other Detectors

Consider:

Proximity and adjacency

What features (location, site, design) pose a threat because they are *near* or *next to* each other?

Consider:

Visibility and Observation

Blind spots, poor lines of sight, obstructions and other features that might pose a threat;

Environmental conditions-- rain, fog, snow-- affect visibility and observation)

Consider:

Continuity

Instances in which continuity of features or systems is interrupted.

Consider:

Condition

Features whose condition pose a potential threat.

Elements of PPS

- Detection
- Delay
- Response

See page D.1 in appendices
(more on this later)

After Lunch

- Assemble at detention facility
- Divide into two groups and tour site
- Use the checklists in Appendix B to prompt you as you observe—
  - B1- Location, Page B1
  - B2- Site, Page B3
- Assemble in new training room to process findings

Take Good Notes

- Good things that you see (strengths)
- Weaknesses that you observe
- Questions that need to be answered in order to determine risk and vulnerability
- **Nothing is too small… remember the chain**

Use your composition book

Step B. Identifying Deficiencies

Facility Design and Layout

- Examining the jail setting from many perspectives to identify concerns
- Using new tools to discover more risks and vulnerability

PHYSICAL CHARACTERISTICS

See Appendix B Checklists:

B3: Facility Design, Layout and Construction (Page B-4)
B4: Video Systems
B5: Alarm and Sensor Systems
B6: Metal and Other Detectors

Consider:

Proximity and adjacency

What features pose a threat because they are *near* or *next to* each other?

Consider:

Visibility and Observation

Blind spots, poor lines of sight, obstructions and other features that might pose a threat;

Environmental conditions-- rain, fog, snow-- affect visibility and observation)

Consider:

Continuity

Instances in which continuity of features or systems is interrupted.

Consider:

Condition

Features whose condition pose a potential threat.

Elements of PPS

- Detection
- Delay
- Response

See page D.1 in appendices
(more on this later)

Next Activity

- Divide into two groups and tour site
- Use the checklists in Appendix B to prompt you as you observe—
  - B3, Page B-6 and those that follow
- Assemble in new training room to process findings

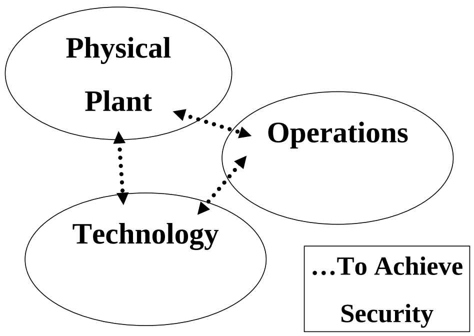
Take Good Notes

- Good things that you see (strengths)
- Weaknesses that you observe
- Questions that need to be answered in order to determine risk and vulnerability
- **Nothing is too small… remember the chain**

Use your composition book

Facility Design and Layout

Remember, It Takes All Three….



Five Focus Areas for Tuesday

- What areas of the facility pose the most risk?

Tonight and Tomorrow

- Reception at B.F. Chaings
- Report here tomorrow at 8 a.m.
- Bring cameras and laptops if you have them

AMERICAN JAIL ASSOCIATION

Calculating Jail Vulnerability

DAY TWO

Madison County
Huntsville, Alabama
May 2008

Sponsored by:

Madison County Sheriff's Office

Today's Agenda

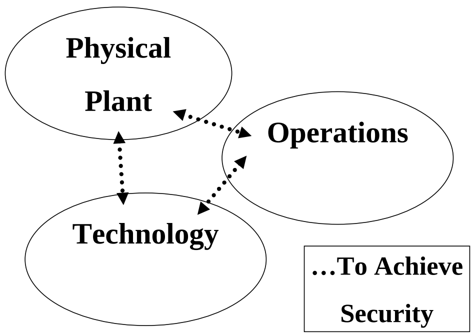
- **Introductions**
- **Quick review of Day One**
- **Assignment to Teams**
- **Assignment to Five Focus Areas (Locations)**
- **Briefings (5) Before Each Round of Site Work**

The Rest of the Week

Wednesday:
- **Assemble initial findings and identify root causes**
- **Begin scenarios and data collection**

Thursday
- **Finish scenarios, analyze with EASI**
- **Present findings**
- **Assemble all findings, develop implementation plans**

It Takes All Three….



Security Principles : Maintaining security is a *continuous* process, demanding sufficient staff who are:

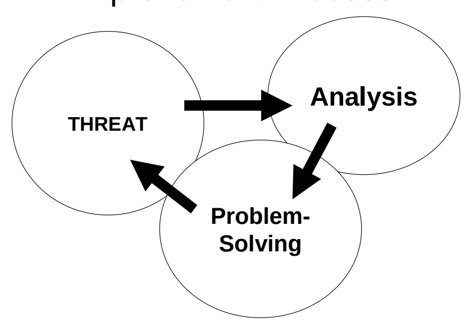
- ❑ qualified,
- ❑ properly trained,
- ❑ directed by policies and procedures, and
- ❑ supervised
- ❑ properly deployed (at the right place, at the right time)

Jail Safety and Security/ Vulnerability Assessment

PROCESS

A. Threat Definition and Capability	
⮟	
B. Identify Deficiencies (combine characterizing and analyzing into a series of excursions into the facility)	
⮟	
C. Assemble Deficiencies and Classify	
⮟	
D. Identify Root Causes ➤	1. ASDs, PSDs Scenarios
⮟	
E. Create Solutions ⮜	2. EASI
⮟	
F. Implement	
⮟ Initial solutions	⮟ Ongoing System

Continuous Safety and Security Improvement Process



Take Good Notes

- Good things that you see (strengths)
- Weaknesses that you observe
- Questions that need to be answered in order to determine risk and vulnerability
- **Nothing is too small… remember the chain**

Use your notebook

Elements of PPS

- Detection
- Delay
- Response

See page D.1 in appendices
(more on this later)

Five Focus Areas

1) Kitchen/Laundry
2) Booking
3) Medical
4) Housing
5) Lobby/Visiting

Threats

- Inmate of Officer Assault
- Contraband
- Escape

Ground Rules

- Be careful– take no risks
- Be discreet- inmates *and others* are watching and listening
- Be especially alert after the VA training
- Take notes
- Take photos, *no identifiable inmates*
- Think like our adversary
- Remember we are in an OCCUPIED and OPERATING facility
- Report serious security breeches to appropriate staff member immediately
- Respect facility staff

Five Rounds of Inquiry

1. Area Checklist (Inventory)
2. Detection
3. Delay
4. Response
5. Operations

1. Area Checklist

- Page 117 of Your Book (Page B-19)

- Layout of Area
- Construction
- Condition

***Layout* of the Area**
Identify potential problems and vulnerabilities that are attributable to the layout of the area, in terms of:
1. Location within the facility:
2. Proximity and/or adjacency (e.g. near rear loading dock, close to fence, etc.):
3. Visibility (is it difficult to see inmates, movement, etc.?):
4. Observation of activities and inmates within the area:

Construction
Catalog the construction of all elements of the area, using the following list as a reference.
Exterior Doors
1. Composition (metal, wood, locks, hinges)
2. Window (size, type of glass)
3. Alarmed (How? Where does alarm record? How is the alarm assessed?)
4. Accessed how? (key opened, electronic, always open, interlocked)

Interior Doors
1. Composition (metal, wood, locks, hinges)
2. Window (size, type of glass)
3. Alarmed (How? Where does alarm record? How is the alarm assessed?)
4. Accessed how? (key opened, electronic, always open, interlocked)

Windows
Composition (glass type, size, bars)
Interior/Exterior?
Walls
Composition (Interior/Exterior)
Ceiling
Composition/Accessibility
Ventilation System
Access Points? (Where does it go? How big? Delays? Composition?)
Utility Chase
Access? (Where does it go? How big? Delays? Composition?)

Ceiling/Roof
Composition.
Access, how? (Be specific. Delay/Detections/Assessment elements)

Condition
Are any physical features in poor repair?
Deteriorating?
Not functioning or not reliable?

Findings

- Record individual notes on site
- Record "ad hoc" observations that might be outside of the focus of the exercise
- Caucus as a team in the training room and assemble all of your responses
- Record your responses in a Word file or on a flip chart (your choice) (including ad hoc)
- Be ready to briefly report your findings to the large group

REPORT
1. Area Checklist

- Page 117 of Your Book (Page B-19)

- Layout of Area
- Construction
- Condition

2. Detection

- Use the checklist on Page 121 of your book (Page D-1)
- Entry controls, key control, etc.
- Perimeter boundaries
- Protection level for infrastructure
- Etc.

•Identify the type of entry control systems in place, i.e. badge, personnel identification, card readers, metal detectors, and state opportunities for piggybacking

•Determine the process for key control, combination locks and seals

•Identify how packages are allowed into the facility, i.e. x-ray, open and visually search

•Documented procedures used to allow access or departure

•Identify and describe the perimeter to include boundaries, fence fabric, gates, sensors (location interior/exterior), length and width of clear zone

A Well-designed PPS:

* provides "protection in depth"

* minimizes the consequences of component failures, and

* exhibits balanced protection.

Performance Criteria Approach

- ❑ Determining how it *really* performs, not what it says on the box (performance-based, not features-based)
- ❑ Required:
  - ❑ Inmate capability
  - ❑ Performance objectives
  - ❑ Effectiveness evaluations
- ❑ Better decision making
  - ❑ Understand effectiveness against specific actions
  - ❑ Effective allocation of resources

A Primer on Physical Protection Systems

88

1. Interior and Exterior Detection Systems

- Introduction
- Sensor fundamentals
- Exterior sensor technologies
- Interior sensor technologies
- System considerations
- Summary

Introduction

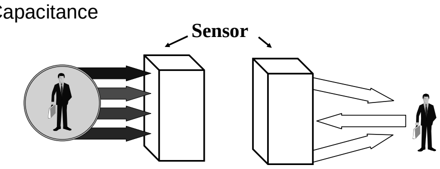
- Physical Protection System Functions
  - Detection
    - Exterior intrusion alarm
    - Interior intrusion alarm
    - Alarm communication and display
    - Assessment
    - Entry control
  - Delay
  - Response

Detection

- Alarm + Accurate assessment = Detection
  - The discovery, by an employee, of an unauthorized Inmate action

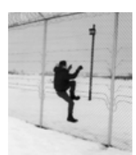
Sensor Classification

- Passive
  - Receiver
    - Vibration
    - Heat(Infrared)
    - Sound
    - Capacitance
- Active
  - Transmitter and receiver
    - Microwave
    - Infrared
    - RF (radio frequency)
    - Other



Performance

- Sensor characteristics
  - Probability of detection, P_D
  - Nuisance alarm rate (NAR)
  - False alarm rate (FAR)
  - Vulnerability to defeat



Exterior Sensor Systems

Intrusion Sensor Technologies

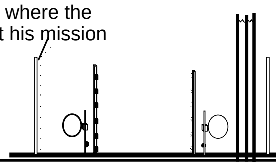
- Microwave
- Active infrared
- Passive infrared
- Buried cable
- Vibration
- Sensor coil
- Taut Wire
- Video motion detectors
- Ultrasonic
- Sonic

Characteristics of an Effective Detection System

- Protection-in-depth
- Minimum consequence of component failure
- Balanced protection
- Integrated with video and barriers
- Clear zone in many cases

Protection-in-depth

- Inmate must defeat or avoid a number of protective devices in sequence
- Protection-in-depth should:
  - Increase inmate's uncertainty about the system
  - Require more extensive preparations by inmate prior to attacking the system
  - Create additional steps where the inmate may fail or abort his mission



Minimum Consequence of Component Failure

- Contingency plans must be provided so the PPS continues to operate after a component fails
- Redundant equipment can take over function of disabled equipment in some cases
- Some failures require aid from sources external to the facility

Balanced PPS

- Provides adequate protection along all possible paths
- Maintains a balance with other considerations
  - Cost
  - Safety
  - Structural integrity

Detection

Sensor Activated ⇨ Alarm Signal Initiated ⇨ Alarm Reported ⇨ Alarm Assessed

- Performance measures:
  - Probability of detection
  - Time for communication and assessment
  - Frequency of nuisance alarms
  - Alarm without assessment is not DETECTION

3. Entry Control and Contraband Detection

101

Objectives:

- Overview of entry control and contraband detection
- Understand contraband detectors

NOTE: this applies to both entry and exit control

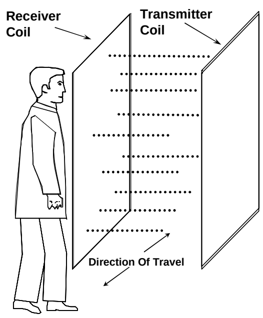
Relative Probability of Detection

• Biometrics and PIN	H
• Exchange picture badge and PIN	
• Exchange picture badge	
• Picture badge and PIN	
• Picture badge	
• Credential and PIN	
• Credential	
• Casual recognition	L

Contraband Detection

- Principles of operation
- Sensitivity factors
- Placement considerations
- X-ray techniques

Coil Geometry for Typical Pulsed Field Metal Detector



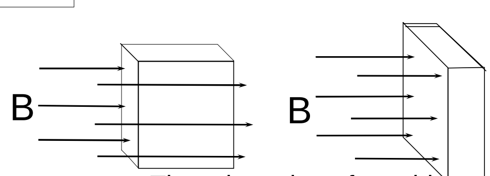
Influences on Metal Detectors

- Objects
  - Weapons
  - Personal possessions
- Detector
  - Type
  - Program
- Walker
  - Velocity
  - Object location

Object Characteristics
- Size & shape
- Orientation
- Type/Metal Combinations

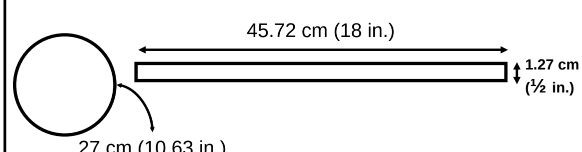
Environment
- Nearby metal
- EM background

Importance of Orientation of Object



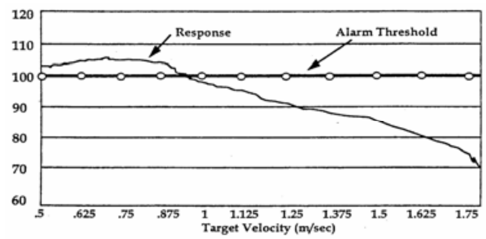
The orientation of an object can change the cross-sectional area that is observed by the magnetic field

Shape



- Two shapes of the same material have equal areas:
  - 58 cm^2 (9 in^2) circle has a circumference of 27 cm (10.63 in.)
  - 58 cm^2 (9 in^2) rectangle has a perimeter of 94 cm (37 in.)
- The resistance of the rectangular path is 3 x higher than the circular path
- **Result: The circle is easier to detect**

Response vs. Target Velocity



CHECKLIST

•Determine the protection level for the security system's infrastructure

•Determine system reliability Ref. B. Equipment and Technical Systems

•Identify the integration between detection and assessment

•Determine the physical and environmental conditions as they relate to PPS

•Past/Present/Future results from known defeat methods, and records related to system

•Performance testing related to assessing situations and emergency incidents

•Identify the present video systems in place and related components (switching equipment/video playback/video monitors/controller/ transmission medium/and monitor location for rapid and immediate assessment)

•Assessment by observation, i.e. CO's in towers, monitoring stations (protection level), and ability to signal duress

•Identify other responsibilities that could reduce assessment capabilities, i.e. respond to alarms, paperwork, and key service

•Identify the information available to the CO on the display board

•Determine the process used in establishing a secondary monitoring station

Findings

- Record individual notes on site
- Record "ad hoc" observations that might be outside of the focus of the exercise
- Caucus as a team in the training room and assemble all of your responses
- Record your responses in a Word file or on a flip chart (your choice) (including ad hoc)
- Be ready to briefly report your findings to the large group

REPORT
2. Detection

- Entry controls, key control, etc.
- Perimeter boundaries
- Protection level for infrastructure
- Etc.

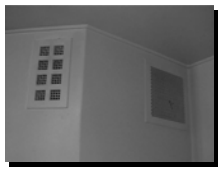
3. DELAY

Page 122-123 of handbook

- Fences/Gates
- Vehicle Barriers
- Walls/windows/doors/roof/floors
- Areas with no detection before delay
- Identify multiple layers of delay

Delay Subsystems

- Passive



Delay Subsystems

- Passive and Active
  - Doors

Delay Subsystems

- Passive
  - Fences

Example Data for Physical Protection System Components

General Task	P_D and Delay Time
Climb 14 ft. fence	20 second delay (climbing)
Running with equipment	10 feet per second
Cut 1 ¾" carbon steel bar with hacksaw	30 seconds per bar
Cut hardened bars with hacksaw	60 minutes per bar
Penetrate cell door without tools	Infinite
Penetrate Metal core door	12 second delay per door
Microwave exterior detection system	0.9 probability of detection
Tilt / vibration fence sensor	0.8 probability of detection
Detectors on building doors	0.99 probability of detection
Interior detector	0.9 probability of detection
Standard deviation on all times	30% of mean

Findings

- Record individual notes on site
- Record “ad hoc” observations that might be outside of the focus of the exercise
- Caucus as a team in the training room and assemble all of your responses
- Record your responses in a Word file or on a flip chart (your choice) (including ad hoc)
- Be ready to briefly report your findings to the large group

REPORT: DELAY

- Fences/Gates
- Vehicle Barriers
- Walls/windows/doors/roof/floors
- Areas with no detection before delay
- Identify multiple layers of delay

4. Response

Page 123 of handbook

- Response force
- Communication available
- Response timeline
- Post and patrol locations
- FAR and NAR
- Armed vs. unarmed
- Diversionary tactics

Response

- Training
- Experience
- Time

Response Considerations

- We will be concerned primarily with the time elements:
  - Who responds and from where?
  - Are weapons carried by on-duty responders?
  - They are often also the assessment – how effective are they at this function and how long does it take?
  - Is the off-site response fast enough to help apprehend the escapees?

Findings

- Record individual notes on site
- Record “ad hoc” observations that might be outside of the focus of the exercise
- Caucus as a team in the training room and assemble all of your responses
- Record your responses in a Word file or on a flip chart (your choice) (including ad hoc)
- Be ready to briefly report your findings to the large group

REPORT: 4. Response

- Response force
- Communication available
- Response timeline
- Post and patrol locations
- FAR and NAR
- Armed vs. unarmed
- Diversionary tactics

5. OPERATIONS

Page 124 of handbook

Protocols (written directions)
Practices (what actually happens)

Are there sometimes differences between what protocols prescribe and what happens on the floor?

Policies and Procedures (Protocols)

- A cornerstone for facility operations
- Describe *IN ADVANCE* what is expected to happen
- Basis for Post Orders
- Foundation for training

PRACTICES

- **Policies and procedures describe what *should* happen**
- **Practices are what actually happen**
- **SECURITY is a continuous process that demands sufficient numbers of staff who are—**
  - **Qualified**
  - **Properly training**
  - **Directed by policies and procedures**
  - **Supervised**
  - **Properly deployed (right place, right time)**

A Resource: Appendix E

- Systematically examine current practices
- Suggest sound practices– a starting point
  - A. Operations
  - B. Equipment and Technical Systems
  - C. Physical Plant

A. OPERATIONS

- A1. Staffing
- A2. Inmate Accountability
- A3. Emergency Preparedness
- A4. Intelligence
- A5. Searches
- A6. Institution Visiting
- A7. Transportation of Inmates (Escorted Trips)
- A8. Security Inspections
- A9. Training

B. Equipment and Technical Systems

- B1. Video Systems
- B2. Alarm and Sensor Systems
- B3. Metal and Other Detectors
- B4. Physical Plant Security
- B5. Perimeter Security
- B6. Locking Systems (Key Control)
- B7. Control Center
- B8. Tool Control
- B9. Utilities and Mechanical Systems
- B10. Toxic/Caustics Control

C. PHYSICAL PLANT

- C1. Location and Site
- C2. Building Layout and Construction
- C3. Entrances and Exits in the Secure Perimeter
- C4. Armory
- C5. Mail Room
- C6. Trash Collection/Disposal

Findings

- Record individual notes on site
- Record “ad hoc” observations that might be outside of the focus of the exercise
- Caucus as a team in the training room and assemble all of your responses
- Record your responses in a Word file or on a flip chart (your choice) (including ad hoc)
- Be ready to briefly report your findings to the large group

REPORT : 5. OPERATIONS

Protocols (written directions)

Practices (what actually happens)

Are there sometimes differences between what protocols prescribe and what happens on the floor?

Wrap Up

- If you have not finished your team notes, please do so before we start tomorrow afternoon (Word or flipchart)
- We start tomorrow at 1 p.m. here, will end by 9 p.m.

AMERICAN JAIL ASSOCIATION

Calculating
Jail Vulnerability

DAY THREE

Madison County
Huntsville, Alabama
May 2008

Sponsored by:

Madison County Sheriff's Office

Today’s Agenda

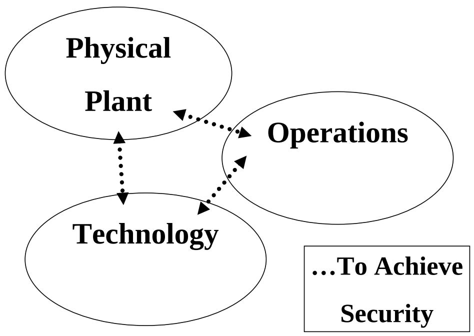
- **Quick review**
- **Assignment of areas to Teams**
- **Finish list of concerns for area**
- **Classify concerns**
- **ID root causes**
- **Begin work on scenarios and EASI worksheet**

The Rest of the Week

<u>**Thursday**</u>

- **Finish scenarios, analyze with EASI**
- **Present findings**
- **Assemble all findings, develop implementation plans**

It Takes All Three….

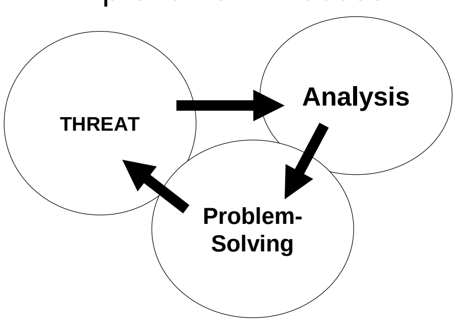


Jail Safety and Security/ Vulnerability Assessment

PROCESS

A. Threat Definition and Capability	
B. Identify Deficiencies (combine characterizing and analyzing into a series of excursions into the facility)	
C. Assemble Deficiencies and Classify	
D. Identify Root Causes	1. ASDs, PSDs Scenarios
E. Create Solutions	2. EASI
F. Implement	
Initial solutions	Ongoing System

Continuous Safety and Security Improvement Process



Five Focus Areas

1) Kitchen/Laundry
2) Booking
3) Lobby/Visiting
4) Housing Floor 1
5) Housing Floor 2

Threats

FOR EASI ANALYSIS:
- Contraband
- Escape

FOR SEPARATE ANALYSIS:
- Inmate of Officer Assault

Ground Rules

- Be careful– take no risks
- Be discreet- inmates *and others* are watching and listening
- Take photos, *no identifiable inmates*
- **Think like our adversary**
- Respect facility staff

A Resource: Appendix E

- Systematically examine current practices
- Suggest sound practices– a starting point
  - – A. Operations
  - – B. Equipment and Technical Systems
  - – C. Physical Plant

A. OPERATIONS

- A1. Staffing
- A2. Inmate Accountability
- A3. Emergency Preparedness
- A4. Intelligence
- A5. Searches
- A6. Institution Visiting
- A7. Transportation of Inmates (Escorted Trips)
- A8. Security Inspections
- A9. Training

B. Equipment and Technical Systems

- B1. Video Systems
- B2. Alarm and Sensor Systems
- B3. Metal and Other Detectors
- B4. Physical Plant Security
- B5. Perimeter Security
- B6. Locking Systems (Key Control)
- B7. Control Center
- B8. Tool Control
- B9. Utilities and Mechanical Systems
- B10. Toxic/Caustics Control

C. PHYSICAL PLANT

- C1. Location and Site
- C2. Building Layout and Construction
- C3. Entrances and Exits in the Secure Perimeter
- C4. Armory
- C5. Mail Room
- C6. Trash Collection/Disposal

ASSIGNMENT

- Review the findings of all teams for your area and discuss
- Go back to your area and find more concerns– of all kinds– and record them on the tables– remember the three threats
- Review your total list of concerns and be ready to report to the large group

CLASSIFYING CONCERNS

- Review each of your concerns/deficiencies
- Determine as a group whether it is:
  - – Facility (physical)
  - – Technical (equipment, technology)
  - – Operational
- Mark your decisions on the table in the appropriate column
- Be ready to summarize to group

Root Causes

- You have been working with "symptoms" so far
- Now it is time to begin to analyze the underlying **causes** as you head toward forging solutions
- Keep asking "why" until you get to the bottom

Find the "root" causes, such as:

- inappropriate *policies* (setting out to do the wrong thing)
- inadequate *procedures* (not attempting to do it the right way)
- training *deficiencies* (not arming staff with the knowledge, skills and abilities they need)

* Supervision: employees actions not being corrected and reinforced by first line supervisors

(continued)

Root Causes (continued)

- *staffing* issues (insufficient staff, wrong type of staff assigned, inadequate deployment, etc.)
- *equipment* shortcomings (the wrong equipment for the application, poor installation, failure to maintain the equipment, etc.)
- *physical plant* problems (poor design, improper construction, inadequate maintenance, etc.)
- **And there are more root causes you will find**

Root Causes

- After you have identified root causes, you will summarize them for the large group
- We will then move into the EASI analysis process, but all of the work you have done up to this point will be combined with the EASI findings tomorrow
- All of your findings will be included in the final report

Path Sequence Diagrams

155

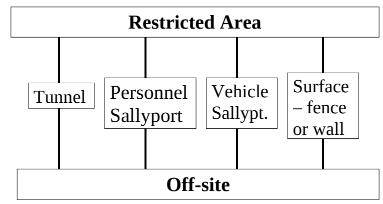
Detection, Delay, Response

- Probability of Detection (P_d): The likelihood, measured as a decimal, that an action will be discovered (detected). Pd of 0.3 means that 30% of the time that action will be detected.
- Delay: The time (measured in seconds) it takes to complete each step in the scenario.
- Response: The time (measured in seconds) it takes an effective responder(s) to intervene after an action is detected.

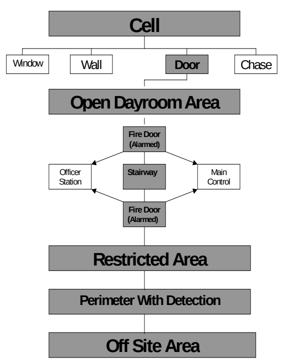
Path Sequence Diagrams (PSDs)

- Graphical model used to help understand the PPS at an institution
- Represent
  - Paths that inmates can follow
  - PPS elements along paths
- Used to determine most vulnerable path for specific PPS and inmate
- Can be developed while touring and/or from institution diagram

Simple Area/Path Sequence Diagram



Sample Path Sequence Diagram



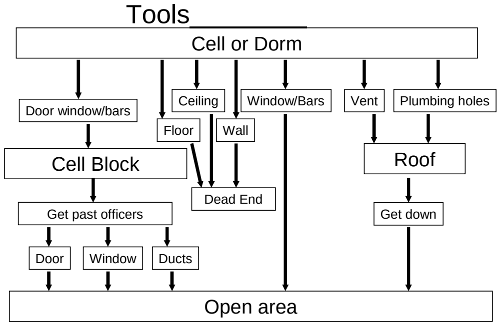
Steps in Constructing PSDs

- **Start with an AREA SEQUENCE DIAGRAM**
- Start where the inmate could start an escape – consider a simple diagram or a list to show the places he/she could start
  - Cell or dorm
  - Kitchen, laundry, work areas
  - Recreation
- Identify all the ways he/she could leave the first area
- Then go to the area outside that one and do the same
- Continue until inmate is outside of the facility

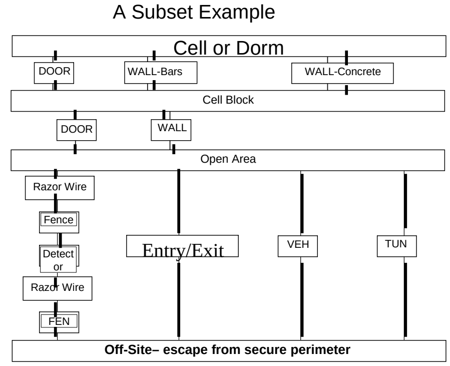
Creating a PSD from an ASD

Time______ Condition ________

Tools__________



A Subset Example

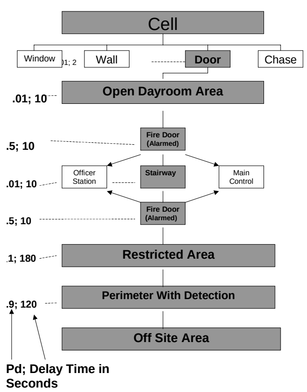


Developing Scenarios

- *Steps for developing scenarios:*
  - Look at the PSD and identify how to defeat each of the security elements.
  - Select the most reasonable defeat or bypass techniques for each of the elements.
  - Establish P_D and delay times for each element for each defeat technique.

Developing Scenarios

- *Steps for developing scenarios:*
  - Add information on the PSD (P_D and delay times).
  - Evaluate the PSD for paths that have low detection.
  - Identify paths that have low delay times.
  - Select a few scenarios for detailed evaluation.



How Do Inmates "Defeat" Us?

- Deceit
- Collusion
- Stealth
- Force
- What are some others?
  ____
  ____
  ____

List Tactics
Cell Example

- Officer opens the cell, the inmate
  – Overpowers officer (force)
  – Sneaks past officer (stealth)
- Get the keys and open the door by
  – Appearing authorized to open the door (deceit)
  – Sneaking up and taking them (stealth)
  – Just taking them (force)

Don't Forget About *Diversions*

- Sometimes inmates create diversions to distract us.
- Inmates sometimes take advantage of incidents and use them as a diversion.
- Be sure that policies and procedures acknowledge this and do not move all staff to respond to the first incident.

Next Steps after Defeat Methods are Identified

- Draw from the details gathered during tours and inspection of documents
  - Type and thickness of relevant barriers
  - Tools that can be used
  - Detection mechanism likelihoods in all areas along the path
  - Average time taken to achieve the action at each element
  - *See checklist in your Handbook*

Develop ***Credible*** Scenarios

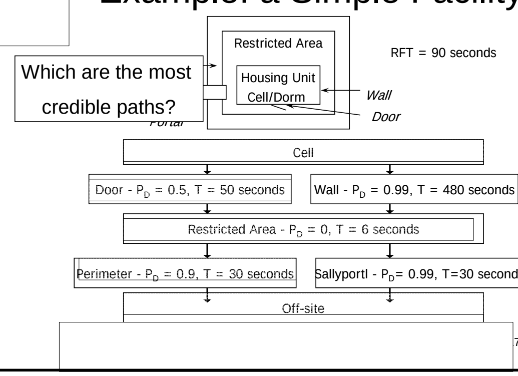
Based on Inmate's Strategy and Element Tactic Lists

- The scenario description is a step-by-step "recipe" for achieving the inmate's goal
- Develop a scenario by "piecing together" what and how the inmate does activities to escape along a defined path
- Consider a range of inmate strategies

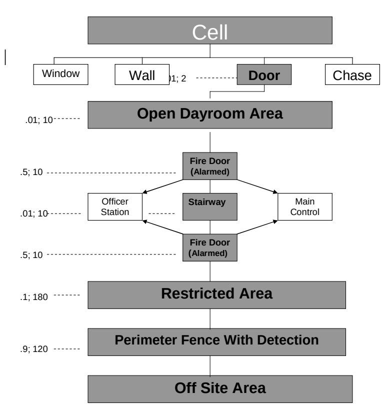
Developing Scenarios

- Evaluate the PSD for paths that have low detection
- Identify paths that have low delay times
- Identify a few credible scenarios for detailed evaluation

Example: a Simple Facility



72



Pd; Delay Time in Seconds

Development of Worst-Case Scenarios

- Create Scenarios
- Assign "Actors"
- Coordinate with Administrative Staff and Shift Commander
- Establish Safety Guidelines/Communications

174

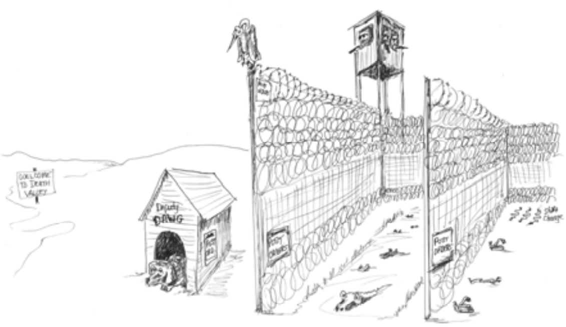
Conduct Performance Testing of Worst-Case Scenarios

❖Assign Test Observers

❖Document Test Results (with Photographs)

Correctional Vulnerability Assessment DATA COLLECTION

176



PROTECTION IN DEPTH.....

Performance Data / Testing

- Purpose
  - Provides data for the analysis
  - Ensures adequacy, functionality, and reliability of system elements or total systems
  - Demonstrates system performance for facility staff with *need* to know
- Can be done by the facility and/or the CVA team

Test Data Collection

- Observation
- On-site surveys
- Subject matter expert interviews
- Published data
- Performance tests

Types of Performance Tests

- *Operability test* - confirms that a system element or total system is *<u>operating</u>*
- *Effectiveness test* - confirms that a system element or total system is functioning as intended

Performance Test Methods

- Limited scope performance test
- Full system exercise
- Quality of these tests will depend on:
  – Detailed planning
  – Comprehensiveness
  – Conditions
  – Recording of results

Planning Performance Tests

- Test scenario development
- Critical issues
- Data collection forms

Number of Tests

- Affects reliability of data
- Based on importance, time required, cost, operational impact
- Frequency of tests

Testing Conditions

- Tests should ideally be conducted under a variety of conditions
  – Varying weather
  – Days of the week, time of day
  – Different shifts
- Experts should determine the relevant conditions and document the rationale for the conditions selected

Performance Data / Testing

- A thorough evaluation of each of these areas:
  – Detection / assessment
  – Delay
  – Response
  – Manufacturer's specifications

Detection/Assessment Data / Testing

- Determine the likelihood of detection for each of the technological sensors
  – Look for dead spots
  – Use common defeat methods
  – Example criteria are in next slides

(continued)

- Determine the effectiveness of personnel in detecting and assessing undesired situations
  - Conduct under various work conditions
  - Simulate situations a number of times

Delay Data / Testing

- Determine the time involved in defeating the walls, windows, doors, roofs, and floors with the inmate capabilities
- Determine the time involved in defeating the fences and gates surrounding the facility with the inmate capabilities
- Evaluate the use of vehicle barriers to determine times they are not effective

Response Force Data / Testing

- Determine the time required to use the type of communication available to officers
- Determine the timeliness of internal communication systems for major events (sirens, duress alarms, PA systems)
- Verify the number and type of primary and secondary responders
- Test all significant elements of the response timeline

Recording Test Results

- Poor recording can:
  - Invalidate test
  - Cause additional testing
  - Portray a false image

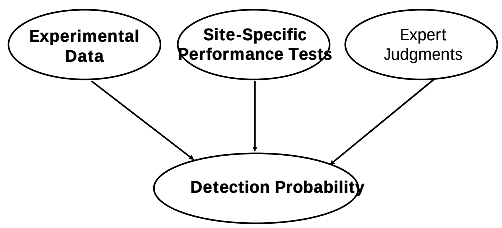
Analyzing Tests Results

- Statistical Analysis
- Validated Expert Judgment
- Expert Judgment

Where do you get this information?

- Your observations while on tour
- Facility documents
- Testing data
- Printed data
- Expert opinion
- All the above data has to be consistent with the defeat approach used by the inmate

Detection Probabilities May Be Obtained From Multiple Sources



Detection at a Barrier

Approximating When Detection Might Occur

- The location of detectors often decides where detection occurs relative to the barrier
  - Before barrier (beginning of delay)
  - On or after barrier (end of delay)
- Probability of detection may increase linearly in time (middle of delay)
- **Beginning, Middle, End**

List Features at Each Path Element --*Inmate Cell Example*

- Wall -12" thick concrete wall with rebar at 6" centers, 4" diameter sewer and water hole, 6"x12" vent with 1/8" grating
- Cell door - two 1/4" steel plates
  - Electronic lock
  - Open cell door sensor
  - 3"x12" Window with one bar
- Personnel generally in vicinity
- Random bed checks by CO's

Example data from testing

Event	**PD and Delay Time**
Doors/Barriers:	
Metal core door with tools	**12 second per door**
30-cm reinforced concrete with tools	**360 second**
1.6-mm doors	**60 second**
Detectors on building doors	**0.99 probability of detection**
Cut 1 ¾ " carbon steel bar with hacksaw	**30 sec. per bar**
Cut hardened bars with hacksaw	**Hrs per bar or infinite delay**
Penetrate cell door without tools	**Infinite**

196

Example data from testing/opinion

Event	**PD and Delay Time**
People:	
Officer at post	0.5 probability of detection
Officer at post	30 second delay
Average CO response time	120 seconds
Running with equipment	10 ft / second

A sample scenario

A composite from several counties

Context

- The female facility is located on a campus with several other facilities
- The control center is in another facility
- Staff is stretched very thin
- There is often only 1 supervisor on grounds for 950 inmates
- Buildings were built for minimum security inmates and now house mediums
- Increase in number of female inmates and seriousness of their offenses
- Jail staff had no input on design
- Due to staffing shortages, the administration decided that it was more important that staff had all the keys in case of emergency response.

Step I

- 2 female inmates wait for a specific officer, (who is small, and was mandated for OT for the 2nd day in a row) to put their plan in action. They wait until meal time, because they know that most of the officers in the female building are busy and assault the targeted officer **and take her keys**.

Step 2

- Because the unit officers all carry handcuffs, the inmates were able to handcuff the officer with her own restraints and lock her in a cell, to delay detection

Step 3

- Inmates unlock Special Management Unit sub day room door and proceed to emergency exit behind the stairs

Step 4

- The inmates find the proper key and unlock the emergency fire door. The door is not alarmed, and the officer had a key to this perimeter door.

Step 5

- The inmates go through the first emergency door and re-secure it so as not to have an officer passing by notice anything out of the ordinary

Step 6

- The inmates then unlock the second emergency door, open it slightly, and look around to see if any staff are present before exiting to the “secure yard”. They believed that it was unlikely that any staff would be present because most of the staff were busy feeding inmates.

Step 7

- The inmates climb over the first of the secure yard fences. The fence has no razor wire, and in the corner the horizontal braces may be used as steps to scale the fence.

Step 8

- The inmates then crawl under the second fence. Due to erosion, there was an 15 inch gap below the fence.

Step 9

- The inmates then proceed to the back corner of the yard where there is no camera coverage, and go under that fence. The ties around the bottom part of the fence were removed by outside conspirators, however, because of the general disrepair, staff didn’t do maintenance checks on the fence.

1. Inmates assault officer and take her keys

- 30 second delay
- .5 probability of detection

DATA COLLECTION

- Delay – Estimate of how long it would take two inmates to overwhelm an officer by surprise. Reach a consensus.
- Pd – Stand in the housing unit during feeding and observe (over several days) how many staff members you see, and what they could see from their positions

2. Officer Restrained with own Cuffs and locked in cell

- 20 second delay
- .5 probability of detection

DATA COLLECTION

- Delay – handcuff someone and place them in to a cell, several times. Take average.
- Pd - By standing on the housing unit during feeding and observing (over several days) how many staff members you see, and what they could see

3. Inmates exit SMU

- 45 second delay
- .5 Probability of Detection

DATA COLLECTION
- Delay – actually walking the distance from the cell to the exit of the SMU, several times, timing it and taking an average.
- Pd - By standing on the housing unit during feeding and observing (over several days) how many staff members you see, and what they could see

4. Inmates unlock emergency door

- 10 second delay
- .5 probability of detection

DATA COLLECTION
- Delay – Timing an "actor" unlocking emergency door, several times.
- Pd – Opening the door while another team member is in the control center observing whether or not the control center operator notices, observing if and how often staff walk by the area. Several times, different staff on shift.

5. Inmates proceed through 1st emergency door

- 10 second delay
- .1 Probability of Detection

DATA COLLECTION

Delay – Time it, several times.

Pd – Observe control and the area several times over several days under several conditions

6. Inmates go through second emergency door

- 10 second delay
- .5 probability of detection

DATA COLLECTION

Delay – time it. Several times.

Pd – Observe control and the area several times over several days under several conditions.

7. Inmates climb over first secure fence

- 10 second delay
- .5 probability of detection

DATA COLLECTION
- Delay – climb over fence several times (or a similar fence if inmate view is an issue) and time it
- Pd – Observe control and the area several times over several days under several conditions

8. Inmates crawl under second fence

- 10 second delay
- .5 probability of detection

DATA COLLECTION
- Delay – climb under fence several times (or a similar fence) and time it
- Pd – Observe control and the area several times over several days under several conditions

9. Inmates go under perimeter fence and escape

- 15 second delay
- .5 probability of detection

DATA COLLECTION

- Delay – climb under fence several times (or a similar fence) and time it
- Pd – Observe control and the area several times over several days under several conditions

EASI%20Simplified%20Version%20Davidson%20CO.%20NEW%20FOLDER[1]

Probability of Interruption:	0.186215995

10	Min Response
300	Max Response

Estimate of Adversary Sequence Interruption

Probability of Alarm Communication		Response Force Time (in Seconds) Mean	Standard Deviation
0.95		200	90

factor 15 >>> 200 >>> max delay

For Instructions, go to the How To Gui

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	(3) Inmates assault officer	0.5	M	30	20
2	IM's restrain officer	0.5	M	20	20
3	Unlock SMU doors	0.5	M	45	20
4	Unlock first emergency door	0.5	M	10	10
5	IM's move through first door	0.1	M	3	3
6	Unlock second emergency door	0.5	M	10	10
7	IM climbs over first dog fence	0.5	M	10	10
8	IM climbs under second dog fence	0.5	M	10	10
9	IM go under perimeter fence	0.5	M	15	15
10					
11					
12					
13					

Probability of Interruption: 18%

Next Assignment

- Create a path sequence diagram for each of your threats. It must contain at least 7 elements (steps).
- Bring your PSD drafts to your honored instructors as they are completed for review and comment.
- Go on site and collect information and data to allow you to insert Probability of Detection, Delay and Response values.
- When done, come to instructors to review work and determine if you may be paroled for the evening.

AMERICAN JAIL ASSOCIATION

Calculating Jail Vulnerability

DAY FOUR

Madison County
Huntsville, Alabama
May 2008

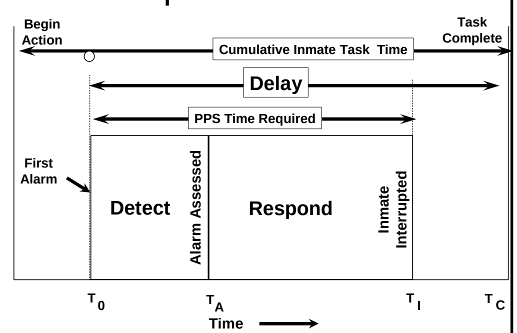
Sponsored by:

Madison County Sheriff's Office

Assessing Risk with the "EASI" Model

221

Inmate Task Time vs. PPS Time Requirements



EASI Analysis Model

- Utilizes the information in the timeline table
- Requires as additional input:
  - Response force time
  - Probability of successful alarm communication
  - Standard deviations on times (usually plus or minus 20% of the value)
  - Location of detection relative to the delay time (Beginning, Middle, End)
- Result is the probability of interruption

Determine RFT

- Response Force Time (RFT) consists of:
  - Alarm assessment time
  - Response communication time
  - Response deployment time
- Can be quite variable depending on the scenario:
  - Accurate assessment is dependent on inmate strategy – hiding vs. actively climbing a fence

Probability of Interruption (P_I)

- Cumulative probability that an officer will interrupt inmate actions before his escape is successful
- The likelihood that an escape will be successful is $1-P_I$, for example:
  - EASI calculates a P_I of 0.6
  - The likelihood of escape is then (1-0.6) or 0.4 [Will be successful 4 times out of 10]

Sample EASI Model - Scenario from a prison

At 1700 hr, an inmate gets to his starting point outside the housing unit undetected. He runs across the outer area to the perimeter fence. Once at the perimeter fence he cuts the razor wire with cutters, cuts the inner fence with cutters, runs across the isolation zone that has a microwave sensor, cuts razor wire on the outer fence, and then cuts through the outer fence. The following EXCEL spread sheet was used to calculate the probability of interruption.

Estimate of Adversary Sequence Interruption	Probability of Alarm Communication	Response Force Time (in Seconds) Mean	Standard Deviation
	0.9	60	5

Task	Description	P (Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Run across outer area	0.1	M	30	5
2	Cut Inner Razor Ribbon	0.1	M	20	3
3	Cut Inner Fence	0.8	M	20	4
4	Run to outer Fence	0.9	M	0	0
5	Cut Outer Razor Ribbon	0.1	M	20	3
6	Cut Outer Fence	0.1	M	20	4

Probability of Interruption:	0.214819151

Likelihood of escape is 0.79

227

Table 2A. EASI Results for Scenario 2 Analysis

Estimate of Adversary Sequence Interruption	Probability of Alarm Communication	Response Force Time (in Seconds) Mean	Standard Deviation
	0.9	75	15

Task	Description	P(Detection)	Location	Delays (in Seconds): Mean:	Standard Deviation
1	Penetrates Exterior Cell Wall	0.5	B	60	12
2	Drop to Restricted Area	0.2	B	10	2
3	Move to Containment Fence	0.2	M	20	4
4	Climb Containment Fence	0.2	M	10	2
5	Move to Inner Perimeter	0.2	M	10	2
6	Cut Shaker Wire	0.3	M	150	30
7	Cut Inner Perimeter Fence	0.1	M	300	60
8	Move through MW Zone	0.8	M	150	30
9	Cut Outer Perimeter Fence	0.4	E	205	41

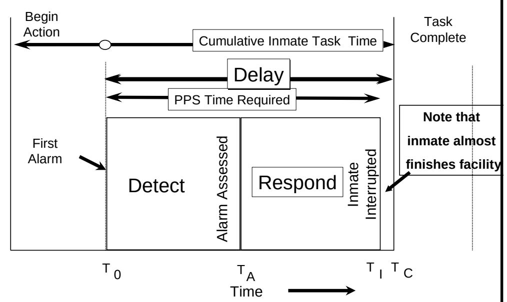
Probability of Int:	0.953746421

Likelihood of escape is 0.05

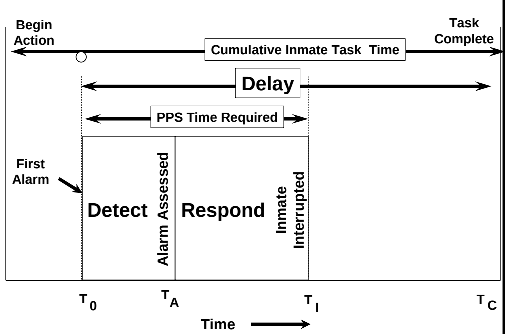
Create a Timeline – Scenario #1

Task Description	PD	Location	Delay time	Stand Dev
Get outside housing unit	.15			
Run across outer area	.3	M	30	7
Cut razor ribbon	.15	M	20	4
Cut inner fence	.4	M	20	4
Run to outer fence	.55	M	8	2
Cut outer razor ribbon	.32	M	20	4
Cut outer fence	.27	M	20	4

Interruption Late in Path



Interruption early in path



Additional information from both the EASI and qualitative analyses

- In scenario #1
  - We only have less than 50 sec. variability in our response time, if we are a bit late the escape will be successful – NOT a very robust system
- In scenario #2
  - We have high detection about 800 sec. before the escape is complete so we have a VERY robust system

232

Formatting Scenario for EASI

Task Description	PD	Location	Delay time	Stand Dev
Get outside housing unit	.15			
Run across outer area	.3	M	30	7
Cut razor ribbon	.15	M	20	4
Cut inner fence	.4	M	20	4
Run to outer fence	.55	M	8	2
Cut outer razor ribbon	.32	M	20	4
Cut outer fence	.27	M	20	4

Let's Do One "Live"

- If you have a laptop, open up the EASI file you loaded earlier and follow along.

Using EASI to Reduce Risk

235

A Reminder…

- Remember to collect all of the seemingly "stray" findings and observations that might not be related to your final scenarios
- Be sure that you do not lose any of these valuable observations when you finish the CVA process.

For each scenario:

- determine the reason(s) for the high level of risk
- evaluate potential options to reduce risk
- consider the cost associated with solutions compared with the benefits

Expand your perspective-

- beyond the high-risk scenarios.
- consider the entire inmate range of inmates and their risk levels
- examine scenarios and situations that are tied into, or which parallel the high-risk scenarios
- identify critical components of the PPS and the extent to which there is defense-in-depth

Think in terms of *systems*

System strengths and weaknesses for *all* types of inmates that will be affected. As you analyze systems, think of:

- safeguards that could potentially enhance protection
- ways to identify and group alternatives to facilitate the meaningful analysis of their benefits
- costs and operational impacts of these upgrade packages

Evaluate Potential Options

- Review security objectives
- Change security system design
- Develop a new design

Final Notes

- Evaluate the costs and benefits for all identified changes and improvements
- Remember that fixing one problem might cause another– be sure everything balances out

241

Creating Your Report

Use Word, Powerpoint, or both

1. Compile your deficiencies, classification, and root causes in a table
2. Describe and illustrate (photos) your scenarios– with Pd and delay for each step
3. Present our EASI findings/table
4. Identify "fixes" identified through EASI
5. Describe findings re: assault on officer (what situations pose a risk to officers?)

Forging Solutions

- Use the table that you started with deficiencies and root causes.
- Add a column describing solution(s) for each issue.
- Identify if the solutions are facility, technical or operational (F,T,O)
- Flag those solutions that involve costs

Be ready to summarize for the group.

IMPLEMENTATION

What thoughts do you have about:

- Initial implementation efforts
- Ongoing safety and security improvement activities

IMPLEMENTATION

PRINCIPLES

- Participation is a key to success
- Consider inviting outsiders as appropriate
- Start with what you have
- Ensure credibility
- Gradual, measured steps
- Empowerment from the top down
- Turn information into data
- Safety and security demand continuous attention

Using a *team* approach:

- * ensures delegation of responsibility
- * provides a diversity of knowledge,
- skills and experience
- * provides the levels of expertise
- needed
- * promotes ownership (especially when
- local facility staff are on the team)
- * speeds up the process

Only the beginning…

- Completing the initial investigation and submitting the report is only the beginning
- Develop an "action plan" with appropriate authorities to address the issues

The "L" Word

- LIABILITY should be considered
- Everyone should do all that they can– within the scope of their power and authority– to address problems
- Document, document, document

"Internal security document"

- Be careful where you circulate the documents
- Many elements of your work should be considered "security documents"
- Political filters might be needed
- Provides a powerful budgeting tool

Policies and Procedures

- Be sure to change policies and procedures as needed
- They might be incorrect or incomplete
- New ones might be needed to address problems

Training

This benefits training in *many* ways—

- ❑Everyone involved received invaluable training and experience
- ❑Staff who observed and learned of findings benefited
- ❑ Findings must be incorporated to ongoing facility training efforts

Supervision

- ❑Many deficiencies may be addressed through improved supervision
- ❑ACA provides new "performance-based" tools to help improve implementation of policies and procedures—
  - ❑Protocols
  - ❑Process indicators
  - ❑Outcome measures

Data and Information

- ❑Data collection activities should continue, and ideally expand and improve
- ❑Create new protocols to fill the data gaps encountered
- ❑Look at the ACA outcome measures for some new ideas

A Vulnerability Assessment is…

- ❑ A *systematic* evaluation in which…
- ❑ Qualitative and quantitative techniques are used…
- ❑ To determine the effectiveness of operational and physical protection systems…
- ❑ Against specific undesired events or a range of potential threats

Is a synthesis

- ❑Provides a multidimensional view, not just one-dimension checklists
- ❑Connects all of the pieces that combine to achieve security
- ❑Offers a new perspective, often from the inmates' point of view
- ❑Often involves actually testing systems, trying scenarios and measuring time frames

Download will Contain:

- Handbook and Appendices
- All Powerpoints used
- Excel file with "EASI"
- Sample CVA Report (from prison)
- All powerpoints developed for CVA
- Work products developed (as appropriate)
- Photos (of group)

Security Principles : Maintaining security is a *continuous* process, demanding sufficient staff who are:

- ❑ qualified,
- ❑ properly trained,
- ❑ directed by policies and procedures, and
- ❑ supervised
- ❑properly deployed (at the right place, at the right time)

Components of a Physical Protection System (PPS)

- Detection
  - The discovery of an inmate action - success depends on detection system effectiveness
- Delay
  - Once the inmate is detected, he must be delayed to allow the corrections officers time to arrive
- Response
  - Consists of actions taken by the corrections officers and other law-enforcement responders to prevent inmate success

Questions

- What more do you need to know now?
- What do you need from us in the future?
- What could we have done better this week?

Please put your word and PPT files onto the flash drive that is circulating, along with photos. Do not take sensitive info with you