FINAL WORKSHOP REPORT

PERIMETER SECURITY STANDARDIZATION

A PUBLICATION OF THE
ANSI HOMELAND SECURITY STANDARDS PANEL

JANUARY 2007

ANSI
American National Standards Institute

STANDARDIZATION FOR PERIMETER SECURITY

WORKSHOP REPORT

Organizer

ANSI Homeland Security Standards Panel (HSSP)

Report publication date

January 2007

More information

www.ansi.org/hssp

ANSI Homeland Security Standards Panel
25 West 43rd Street – Fourth Floor
New York, NY 10036
T: 212.642.4992
F: 212.398.0023
E: mdeane@ansi.org

TABLE OF CONTENTS

Introduction

This Workshop report seeks to provide guidance and assistance to standards developing organizations (SDOs) who are involved with standards activity for various aspects of "perimeter security," in the context of homeland security and homeland defense. This report does not look to provide the business case for the development of perimeter security standards, but rather addresses the key issues and elements that should be considered in this standardization area.

The primary focus of this report is on securing the perimeter of various "security interests" (i.e., potential targets) from intentional attacks (*e.g.*, from premeditated attacks by terrorist groups). The focus is not on establishing standards for perimeter security for the primary purposes of safety or for preventing trespassing or ordinary crime (*e.g.*, theft, vandalism, etc.). However, it is recognized that perimeter-security actions taken for homeland security/defense purposes are likely to serve other safety and security-related purposes.

Following the summary of the ANSI-HSSP Workshop proceedings, this report is organized into three general sections. The first section presents some basic concepts and definitions, intended to improve the clarity and precision of the following analysis and discussion. Specific concepts such as security interests (potential targets), target perimeter, security perimeter, perimeter security, attacks and threats, and risk are addressed.

The second section of the report builds from the first and presents several models which, taken together, provide a general conceptual framework for considering the need for, and nature of, standards for perimeter security. In particular, these models address the variable nature of U.S. security interests (potential targets) and the range of threats to those security interests, especially the range of intentional attack scenarios. They also address the topic of perimeter security in the context of the current U.S. national homeland security policy that takes a risk-management approach and incorporates a "layered-defense" strategy, involving threat identification, prevention, consequence mitigation, emergency response, forensics and attribution, and recovery and reconstitution.

Using the foundation presented in the first two sections, the final section presents a number of specific issues, factors and recommendations that SDOs should consider, in developing perimeter-security standards. This discussion recognizes the complex, wide-ranging and variable nature of perimeter security applications and that ultimately, the “global standard” to be met by any particular perimeter-security system is that it be tailored to, and optimized for, the specific situation in which it is to be employed.

Acknowledgement and sincere appreciation is given to Dr. Todd Stewart, Major General, United States Air Force (Retired) and Director, Program for International and Homeland Security, The Ohio State University. Dr. Stewart authored the white paper that captured the key points of the perimeter security dialogue and which served as the foundation for this Workshop report.

ANSI-HSSP Workshop Proceedings

The ANSI Homeland Security Standards Panel (HSSP) has as its mission to identify existing consensus standards, or if none exists, assist the U.S. Department of Homeland Security (DHS) and those sectors requesting assistance to accelerate development and adoption of consensus standards critical to homeland security. The ANSI-HSSP promotes a positive, cooperative partnership between the public and private sectors in order to meet the needs of the nation in this critical area. To address specific homeland security standards areas, Workshops are convened under the ANSI-HSSP to bring together subject matter experts in that particular security area.

During the December 13-14, 2004 Panel plenary meeting, the subject of enterprise power security and continuity was endorsed as one of two new areas to be explored via workshops due to its importance to homeland security.

On May 17, 2005, a Perimeter Security Summit was convened in Washington DC. The Summit was focused on the near-term practical challenges and emerging solutions relating to perimeter security for critical facilities. The Summit also addressed security technologies and systems needed to complement and enhance guards, gates, and personnel verification. The agenda for this well-attended Summit addressed the following major areas:

- Civilian Targets on the Front Line
  Technology convergence: military, homeland, private sector

- Real-World Examples: Federal and DoD Perimeter Protection
  Military bases, airports, harbors, embassies and government buildings – at home and abroad. What works today, who provides it, what it costs, what's needed next?

- Expanding the Perimeter
  Technology as a "force" multiplier for guards and gates, enhancing situational awareness – long-range sensing, seeing, tracking

- Guarding Portals – Sensing Invisible Threats
  Detecting explosives, chemical, biological, and radiological hazards

- Integrating & Synthesizing
  Systems integrating of perimeter security data and communication

Following the Summit, the ANSI-HSSP Workshop was convened to address the issue of standards for perimeter security. Organizations that were represented at this May 2005 meeting can be found in Annex A. The majority of the workshop meeting was spent discussing user needs for standards in the area of perimeter security and the key issues and challenges that should be considered when tackling this subject. Volunteers were identified at the meeting to serve on a task group to further examine the role for standards and conformity assessment programs.

Through its further investigation and deliberations, the task group confirmed that perimeter security standardization is a complex area to address. Elements that make this a complex issue included the multiple ways of defining the perimeter (person, building, city, trucks/railway cars carrying chemicals to and from chemical plants, etc.), how some perimeters are inherently open (*e.g.*, airport) and others are inherently closed (*e.g.*, chemical plant), and how different perimeters have different acceptable levels of security (and expectations from the customer).

Despite the complex subject area, the task group agreed to two main principles, which are reflected throughout the remainder of this Workshop report:

1. Perimeter security standards need to be outcome focused (i.e., performance of the entire system as opposed to simply the components themselves).
2. Perimeter security standards need to be risk-based.

With these two principles in mind, the task group considered a three-dimensional matrix for capturing standards related to perimeter security and identifying gaps. While the matrix proved a useful way to visualize the situation (see *Figure 12* in this report), in practice it proved too difficult to populate with standards. Another consideration was to have the task group simply track existing standards and gaps for the components of perimeter security (cameras, guard force, barriers, etc.), but this approach was questioned due to the ambiguity of all the areas/items that could be defined as components of perimeter security and because it deviates from the 'performance of the entire system' approach.

The task group decided that without the directive from some authority requesting a specific aspect of perimeter security standardization be analyzed, the overall area of perimeter security is too big and too generic to provide a detailed inventory of existing standards and gap areas. In place of this inventory of standards, the task group decided to produce this three-section report as outlined in the Introduction, with the hopes that it will provide some useful guidance to those organizations involved with writing and utilizing perimeter security standards.

Concepts and Definitions for Perimeter Security

One of the challenges in developing perimeter security standards is to evolve a common understanding of basic terms and concepts. A review of current publications dealing with "perimeter security" will reveal a lack of consistency in the use of basic terms, resulting in the potential for considerable confusion and miscommunication. Consequently, some basic definitions and concepts are offered.

U.S. Security Interest

In the broadest context, a security interest refers to anything that has value as a potential "target" of an intentional attack. Security interests can include:

- Tangible/physical interests:
  - Individuals
  - Permanent concentrations of people (*e.g.*, cities) or temporary groups of people (*e.g.*, concerts, athletic events, etc.)
  - Physical (critical) infrastructure and key assets, naturally-occurring or man-made; fixed or mobile. For example, the National Infrastructure Protection Plan identifies the following categories of critical infrastructure:
    - Agriculture
    - Food
    - Water and Wastewater
    - Public Health and Healthcare
    - Emergency services
    - Government
    - Defense Industrial Base
    - Information Technology
    - Telecommunications
    - Energy
    - Commercial Nuclear Reactors
    - Dams
    - Transportation
    - Banking and Finance
    - Commercial Facilities
    - Postal and Shipping
    - Monuments and Icons
    - Chemical Infrastructure
- Intangible/non-physical Interests:
  - Societal values (*e.g.*, the concepts and freedoms described in foundational documents such as the U.S. Constitution, as amended; Declaration of Independence; etc.)

For purposes of this report, focus is primarily on those tangible/physical security interests, which serve as the basis for defining a "perimeter." Also, this report focuses primarily on fixed (vice mobile) security interests, recognizing that it is possible (and necessary) to expand the discussion to include the perimeter and perimeter security of mobile targets, as well.

Boundary
A boundary (or target boundary) is the extent or limit of a security interest (potential target) in a particular direction, horizontally or vertically. A boundary can be either permanent or temporary and can be defined or marked in a number of ways, *e.g.*, by a physical feature of some type, either naturally occurring or man-made, or by a non-physical description. Examples include:

- Physical boundaries: coastlines, rivers, fences, walls, roads, etc.
- Non-physical boundaries: legal limits of real-property ownership, limits of political jurisdictions, etc. Non-physical boundaries can also define areas that are legally zoned or restricted for purposes of safety, public health, environmental protection, economic development, etc., *e.g.*, U.S. air space or U.S. territorial waters.

Perimeter
A perimeter (or target perimeter) is a natural, defined or constructed set of boundaries that, when taken together, completely surrounds or encloses a particular security interest or potential target. Perimeters, like boundaries, can be either permanent or temporary. For example, the perimeter of the continental United States is collectively defined by the following boundary segments:

- Atlantic coast (extended to the limit of U.S. territorial waters)
- Gulf of Mexico coast (extended to the limit of U.S. territorial waters)
- U.S.-Mexico border
- Pacific coast (extended to the limit of U.S. territorial waters)
- U.S.-Canada border
- U.S. air space over the continental U.S.

A perimeter can also be a set of boundaries that completely encloses a threat to a particular security interest that lies outside of the perimeter, as in the case of a prison or an area of public-health quarantine.

Security Perimeter:
A perimeter of a particular security interest or potential target that is to be secured as a defense against an attack. In this context, a security perimeter can be inside of the target (territorial) perimeter of the security interest, coincident with it, or outside of the territorial perimeter. For example, some very large military reservations have security perimeters established well inside of the (real-estate) perimeter of the installation. On the other hand, inspecting cargo containers bound for the U.S. at the foreign ports of embarkation is an example of extending the security perimeter beyond the territorial (target) perimeter. In another example, the security perimeter for a commercial airport may need to be established well outside the real-estate perimeter of the airport, to deal with the threat of attacks with shoulder-fired missiles.

Perimeter Security System: This refers to the system of people, technologies, geophysical features, processes and operations employed to secure a particular security interest (potential target) from unauthorized access, particularly premeditated attacks intended to injure, damage, destroy, or impede the normal operations of the security interest. Perimeter security system components include the system's subsystems or system elements, commonly:

- Security forces (people, weapons, vehicles, etc.)

- Barriers and gates
- Lighting
- Sensors
- Warning devices
- Other active and passive systems (lethal and non-lethal), *e.g.*, anti-personnel mines, etc.
- Personnel identification systems
- Command, communication and control systems (the mechanism by which the various components of the system are integrated and coordinated)

Perimeter-security systems might also include software that provides the "firewalls" and other cyber-security measures for information systems that are security interests.

Perimeter Security System Design

This refers to the process – and the result of the process – to establish the system's:

- Performance goals and characteristics (system performance criteria and related standards)
- System Elements
  - Components (i.e., component types, quantities, performance characteristics, etc.)
  - Configuration (how the components relate to, and interact with, one another)
- Processes (how the system works)

Perimeter Security (or Perimeter-security System Effectiveness)

This refers to the effectiveness of the perimeter-security system in:

- Deterring attacks;
- Detecting and identifying or characterizing a particular threat or set of threats to the security interest (potential target) being secured by the system;
- Protecting the security interest from particular threats or modes of attack;
- Mitigating the damage or disruption, resulting from an attack; and (in some cases)
- Neutralizing, defeating, capturing and/or destroying the attackers.

This also refers to the system's "functionality," meaning how well the system performs its intended purpose or function.

Attack

As used in this paper, an attack (or attack scenario) refers to a *terrorist act*, i.e., a premeditated act of violence or threat of violence; perpetrated by some hostile individual, (non-state) group, or foreign government; directed at some security interest or target (people or property); intended to accomplish political, religious, ideological or other objectives; by influencing some intended audience through intimidation, coercion or fear. An attack can be described by (at least) three components:

- Characteristics of the attackers (e.g., numbers, leadership, motivation, planning, resources, technical competency, etc.)
- Objectives of the attack (e.g., operational disruption, economic impact, casualties, etc.)
- Mode of attack (e.g., type and numbers of weapons used, methods of employment, etc.)

Threat

The term “threat (or attack threat),” as used in this discussion, refers to the probability that a specific attack (attack scenario) will be directed at a particular target or security interest.

Target Vulnerability

The susceptibility of a particular security interest (potential target) to a specific attack scenario.

Attack Consequences

The adverse impacts (outcomes) resulting from a particular (successful) attack on a specific target, fatalities and injuries; short- and long-term health impacts; infrastructure damage or destruction; disruption of essential services; near- and long-term economic losses; political and societal impacts; etc.

Risk

The risk of a particular attack scenario directed at a specific target is a function of three general factors:

- Threat
- Target Vulnerability
- Attack/event Consequences

Perimeter-Security System/Component Performance Criteria

The various measures (or scales of measurement) used to assess the performance of a particular perimeter-security system or system component. Examples of possible (general) perimeter-security system/component performance criteria include:

- Effectiveness (functionality)
- Efficiency
- Reliability
- Maintainability
- Sustainability
- Flexibility (adaptability)
- Durability
- Resilience
- Affordability

To be usable in practice, each of these criteria must be “operationally defined.” An operational definition is simply the scale of measurement used to assign quantifiable values to the criterion. For example, reliability is commonly measured as the percentage of the time a system (component) is operating as designed, during a specified time span.

Perimeter-Security System/Component Performance Standards
For each perimeter-security system/component performance criterion of interest, the "standard" is the target/desired value of the criterion's operational definition, typically a maximum or minimum value. In the case of the reliability example (above), the standard might be specified as, "at least 0.999."

Conceptual Framework for Perimeter Security

Before addressing the specific factors and issues that need to be considered in developing perimeter security standards, it is useful to have a conceptual framework that helps to put perimeter security and perimeter security systems into the context of homeland security. This section offers such a general conceptual model, using the basic concepts and definitions presented in the previous section.

As Figure 1 illustrates, the model begins with an understanding of security interests, i.e., those people or things that are potential targets and which we wish to secure:

Homeland-Security Strategic Model

Homeland Security Interests (Targets)

Figure 1: Homeland-Security Interests

General examples of U.S. homeland security interests (potential targets) that might be the object of perimeter security include:

- The nation as a whole, where U.S. borders (and airspace) collectively represent the nation's perimeter;
- People (*e.g.*, prominent individuals; permanent and temporary groups)
- Buildings (commercial, institutional, residential)
- Installations or communities (collections of people, buildings and activities)
- Other structures in the built environment (*e.g.*, dams and locks, utility and communication systems, bridges, tunnels, port facilities, power plants, etc.)
- Monuments and national icons
- Concentrations of key natural resources
- Linear systems (*e.g.*, pipelines, energy-transmission lines, rail lines, highways, etc.)
- Mobil systems (*e.g.*, aircraft, ships, trains, subways, buses, trucks, etc.)

When considering potential threats to U.S. homeland-security interests, the current national homeland-security strategy takes an "all-hazards" perspective, as illustrated in Figure 2:

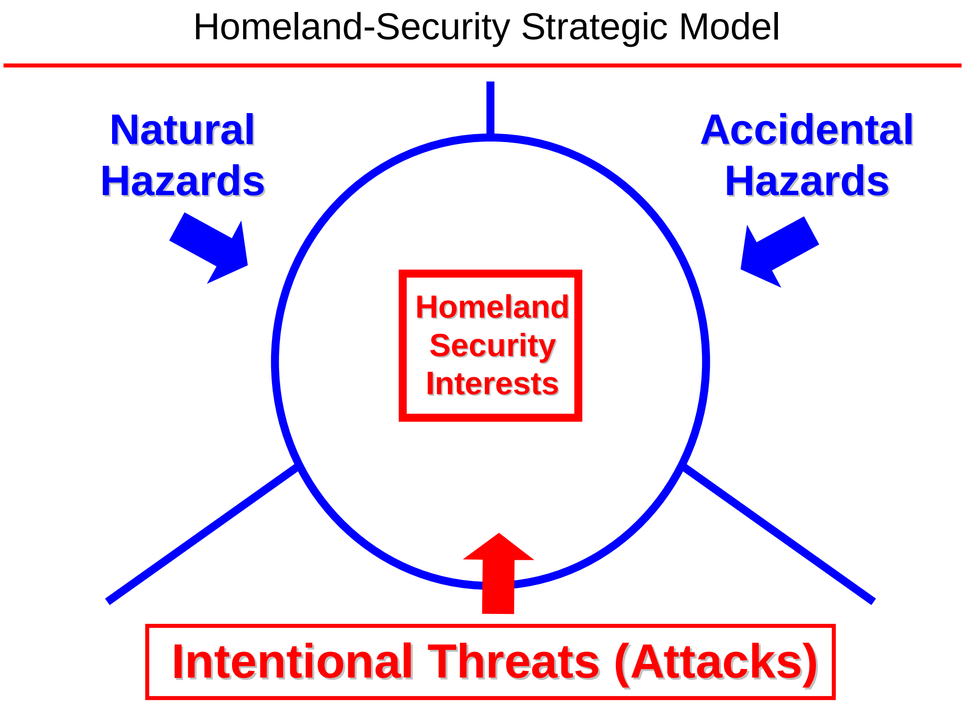

Homeland-Security Strategic Model
Natural Hazards
Accidental Hazards
Homeland Security Interests
Intentional Threats (Attacks)

Figure 2: An "All-Hazards" Perspective

For purposes of this discussion, we are focused on intentional, premeditated attacks on U.S. homeland security interests, by individuals, non-state groups, or other countries.

The nature of the actions and capabilities required to adequately secure a potential target (including providing perimeter security) depends on the threat (likelihood) of a particular attack scenario directed against a target, the vulnerability of the target to that type of attack, and the consequences of the attack, if successful. As noted in the previous section, a particular attack scenario can be described by the characteristics of the attackers, objectives of the attack, and the mode of attack.

Figure 3 illustrates one alternative (simplistic) scheme for generally characterizing attack scenarios:

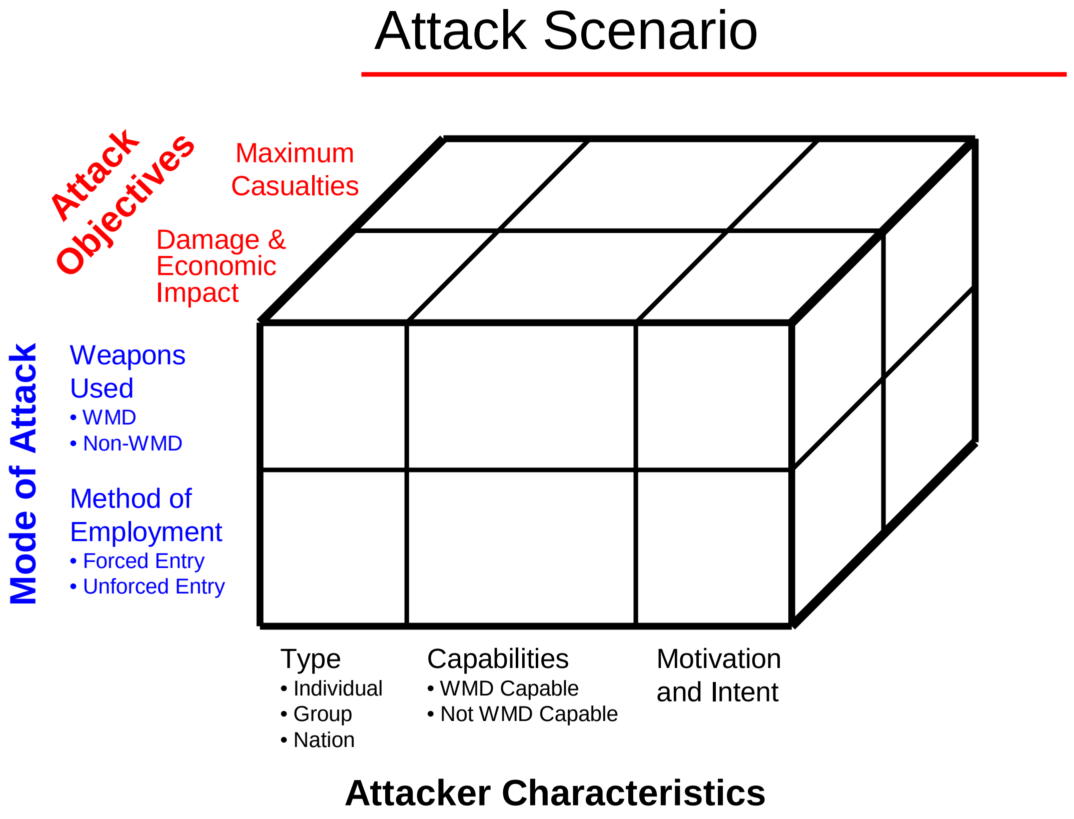
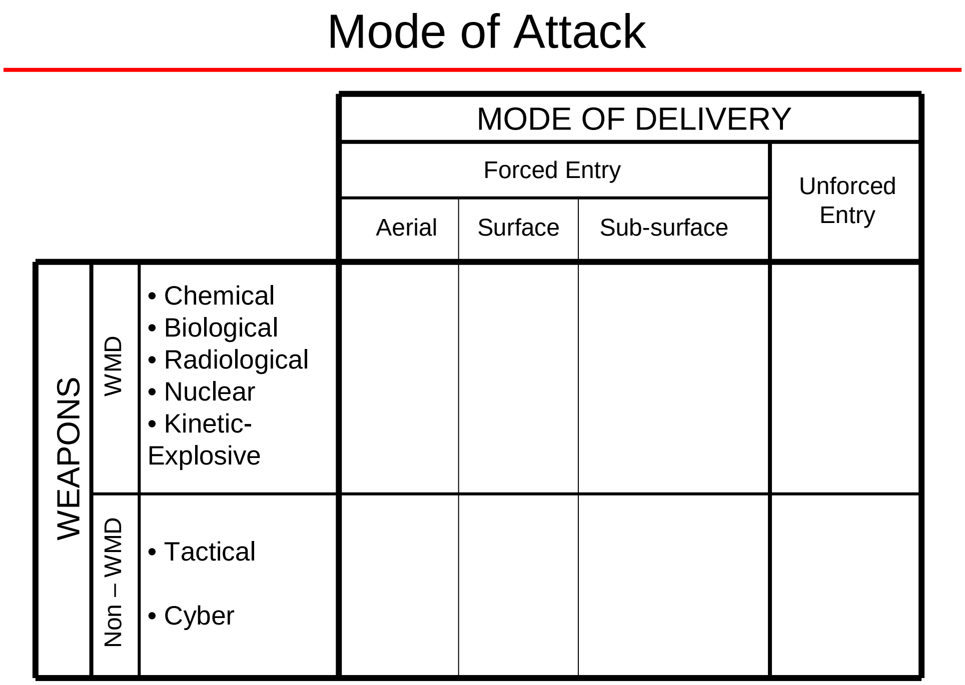


Figure 3: Attack Scenarios

Each of these components can be further developed to provide additional specificity. Figure 4 expands the characterization of the "Mode of Attack."



Mode of Attack

			MODE OF DELIVERY			
			Forced Entry			Unforced Entry
			Aerial	Surface	Sub-surface	
WEAPONS	WMD	• Chemical • Biological • Radiological • Nuclear • Kinetic-Explosive				
	Non – WMD	• Tactical • Cyber				

Figure 4: Mode of Attack

The characterization schemes illustrated in Figures 3 and 4 are meant to be illustrative, not definitive. The point is that the most cost-effective strategy for providing adequate security to a particular target, including adequate perimeter security, will depend significantly on the nature of the target and especially, on the attack – and the threat (probability) of such an attack.

Figure 5 expands the conceptual model by illustrating the general strategic process for securing any potential target against an attack, as well as responding to, and recovering from such an attack. It also illustrates (in general terms) how perimeter security contributes to the overall strategy. Specifically, the primary value of perimeter-security actions is in protecting and defending the target from attacks that cannot be deterred or pre-empted. However, as the model indicates, a strong perimeter security can also contribute to deterrence and recovery.

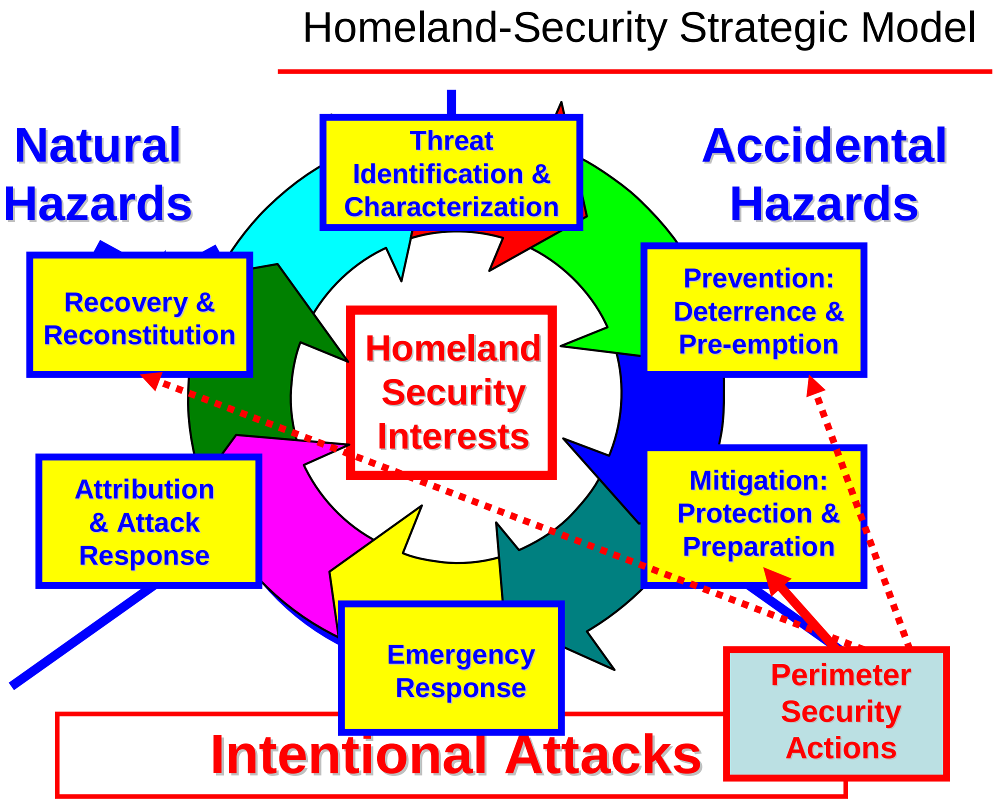

Homeland-Security Strategic Model
Natural Hazards
Accidental Hazards
Threat Identification & Characterization
Prevention: Deterrence & Pre-emption
Mitigation: Protection & Preparation
Emergency Response
Attribution & Attack Response
Recovery & Reconstitution
Homeland Security Interests
Perimeter Security Actions
Intentional Attacks

Figure 5: Strategic Security Process

For each step in the strategic security process, including determining appropriate perimeter-security actions, it will be necessary to:

- Prescribe the goals or objectives to be achieved, i.e., the desired effects or outcomes; and
- Identify the capabilities (processes, technologies, resources, etc.) necessary to achieve the desired effects or outcomes, ideally, at the lowest total cost of ownership. In the context of this report, if perimeter security is part of the overall security strategy for a particular target-attack scenario, one needs to determine the most cost-effective perimeter-security system, which implies the need to specify system (and component) performance criteria and associated standards.

The current national strategy for homeland security is predicated on the realization that it is impossible to be totally secure, i.e., it is not possible to totally eliminate the risk of (all) intentional attacks on (all) U.S. security interests. Consequently, the nation has adopted a national homeland-security strategy of attempting to manage the risk. This strategy also recognizes that risk-reduction strategies are not free; there are costs: financial, social, and political. So, in effect, the national strategy for homeland security is one of managing the risk and the associated costs for various potential threats to U.S. security interests. This strategy is illustrated graphically by the influence diagram shown in Figure 6.

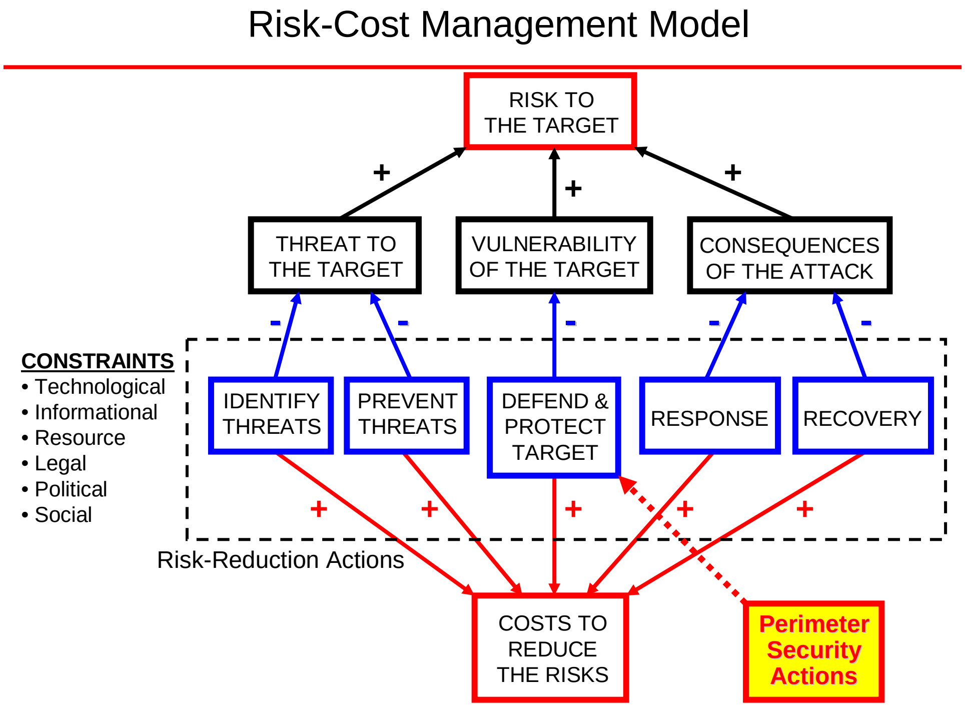


Figure 6: Risk-Cost Management Model

(Note: In this influence-diagram model, the "+" refers to a direct relationship and the "-" refers to an inverse relationship.).

Figure 6 also highlights the important point that various risk-reduction strategies are likely to involve a combination of actions taken to reduce the threat, vulnerability and/or consequences of an attack. Actions taken to improve perimeter security can have a deterrence effect, as well as defending the target from an actual attack. To the extent perimeter-security actions mitigate the damage done by an attack, they also contribute to reducing the post-attack actions required to recover and reconstitute the target. Finally, Figure 6 illustrates the important point that any particular risk-reduction strategy will be determined by a number of constraints or limiting factors.

Figure 7 illustrates a notional risk-cost curve for the model in Figure 6. In this case, the curve represents the most cost-effective feasible strategy for achieving any acceptable level of risk (of a particular type of attack on a specific target) and the associated cost. Since risk is a function of threat, vulnerability and consequences, each point on the curve represents the most cost-effective set of values for these three variables. By comparing the values of threat, vulnerability and consequences for the current level of risk (point A in Figure 7) with the corresponding values for the allowable or acceptable level of risk (point B in Figure 7), one can determine the most cost-effective strategy for reducing risk. If, for example, the most cost-effective risk-reduction strategy involves improving perimeter security (or perimeter-security system effectiveness) by some amount, the model should also suggest (in theory) what specific changes should be made to the perimeter-security system.

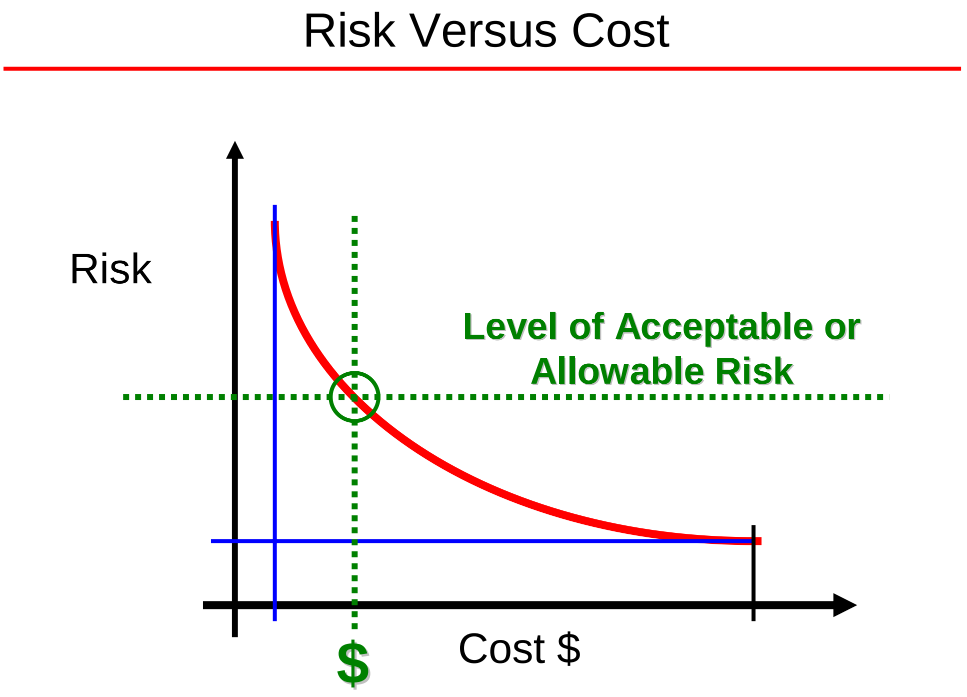


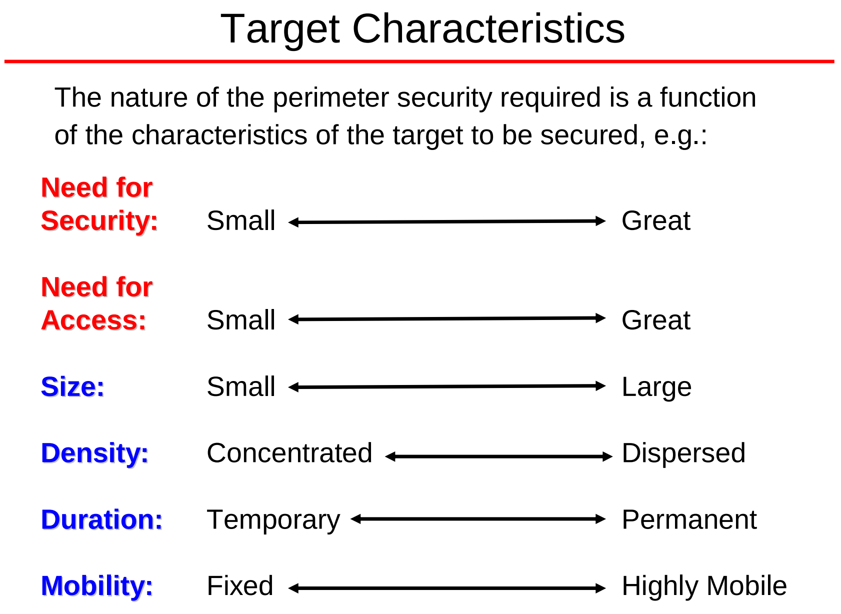
Figure 7: Risk-Cost Policy Curve (notional)

Considerations for Developing Perimeter Security Standards

The basic concepts and definitions presented in the first section of this report and the conceptual models described in the second section were intended to provide a foundation for a discussion of factors and issues that need to be considered by organizations responsible for establishing standards related to various aspects of perimeter security. There are a number of specific factors and issues that should be considered.

- The need for perimeter security and perimeter-security systems, and the nature of those systems, is a function of:
    - The characteristics of the target;
    - The current and projected threat or set of threats to that target; and
    - The role and value of perimeter security in the context of the overall security strategy for dealing with anticipated threats to the target.

- Figure 8 illustrates the point that the nature of any particular perimeter-security strategy and system (i.e., its configuration, operational processes, etc.) will depend in part on the characteristics of the security interest, *relative to the nature of anticipated threats.* Two characteristics are particularly influential: (1) the need to secure the target (a function of the consequences of a successful attack of some type), and (2) the need for convenient access to the potential target for the effective and efficient accomplishment of its mission. Figure 9 further illustrates this point by arraying a number of notional examples in a graph defined by these two dimensions.



Target Characteristics

The nature of the perimeter security required is a function of the characteristics of the target to be secured, e.g.:

Need for Security: Small ↔ Great

Need for Access: Small ↔ Great

Size: Small ↔ Large

Density: Concentrated ↔ Dispersed

Duration: Temporary ↔ Permanent

Mobility: Fixed ↔ Highly Mobile

Figure 8: Target Characteristics Affecting Perimeter security

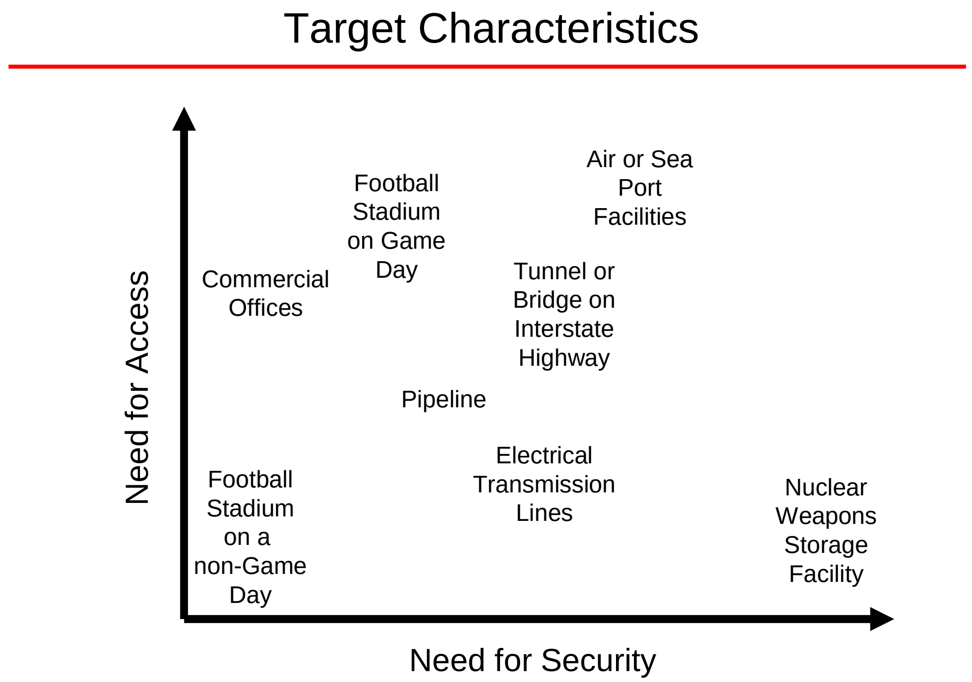

Target Characteristics
Need for Access
Need for Security
Air or Sea Port Facilities
Football Stadium on Game Day
Commercial Offices
Tunnel or Bridge on Interstate Highway
Pipeline
Electrical Transmission Lines
Football Stadium on a non-Game Day
Nuclear Weapons Storage Facility

Figure 9: Examples Arrayed by Need for Access versus Need for Security

- Since both the nature of the target and the threats to that target are inherently variable over time, the most cost-effective overall security strategy is also most-likely variable, as is the need for, and the nature of, perimeter-security systems, as a component of the overall security strategy. Highly dynamic target-threat situations will require highly-flexible and adaptive security strategies, potentially including perimeter-security systems that are also very flexible and adaptive. Conversely, for target-threat situations that are relatively stable and predictable, strategy and system flexibility/adaptability is (relatively) less important.

- The specific nature of a perimeter-security system (if required as an element of the overall security strategy) will also depend on the purpose of the system. The nature of a perimeter-security system that is intended to deter, detect, defend against, and mitigate the consequences of a forced-entry attack against a specific target will likely be different from a perimeter-security system that is also intended to capture and/or destroy the attackers (not just fend off the attack).

- The general goal in designing the most appropriate perimeter-security system for any particular target-threat scenario is to determine the system that provides the required degree of perimeter-security effectiveness (in the context of, and relative to, the overall security strategy), while complying with all applicable constraints (e.g., operational, technological, resource, informational, political, legal, societal, environmental, economic, etc.), at the minimum total cost of ownership (i.e., total life-cycle cost). *Consequently, the overall or "global standard" for perimeter-security systems is that these systems have been optimized for the particular situation in which they are intended to function*.

- Designing the most appropriate perimeter-security system for any particular target-threat scenario can be facilitated by considering the following questions:
    - What is the acceptable level of risk (of a particular type of attack against the specific target or security interest)? In this context, "risk" can also be thought of as the expected value of the consequences of a successful attack.
    - What is the current level of risk and how is that risk projected to change in the future?
    - If the current (and/or projected future level of risk) exceeds the allowable or acceptable level of risk, what is the most cost-effective, feasible, overall risk-reduction strategy? What actions should be taken to reduce the threat, the vulnerability and/or the consequences of the anticipated type(s) of attack against the target?
    - If those general-strategy actions involve (or possibly involve) establishing a perimeter-security system or improving the performance effectiveness and/or efficiency of an existing perimeter-security system, what level or degree of perimeter-security system effectiveness and/or efficiency is required? In other words, what is the standard for perimeter-security system effectiveness and/or efficiency in the overall security strategy?
    - What is the current level of perimeter-security system effectiveness and/or efficiency, relative to the standard or goal?
    - If the current level of perimeter-security system performance does not meet the standard or goal, what specific changes need to be made to the perimeter-security system to achieve the desired system performance standard(s), while complying with all applicable constraints, at the lowest total cost of ownership?
        - What changes need to be made to system components (i.e., changes to component type, quality, quantity, etc.), e.g.:
            - Warning systems and devices
            - Barriers and gates
            - Sensor systems
            - Lighting
            - Response forces
            - Personnel identification systems
            - Other active and passive systems
        - What changes need to be made to the manner in which these various subsystems and components are configured, integrated, coordinated, commanded and controlled?

The influence-diagram model Figure 10 illustrates these relationships:

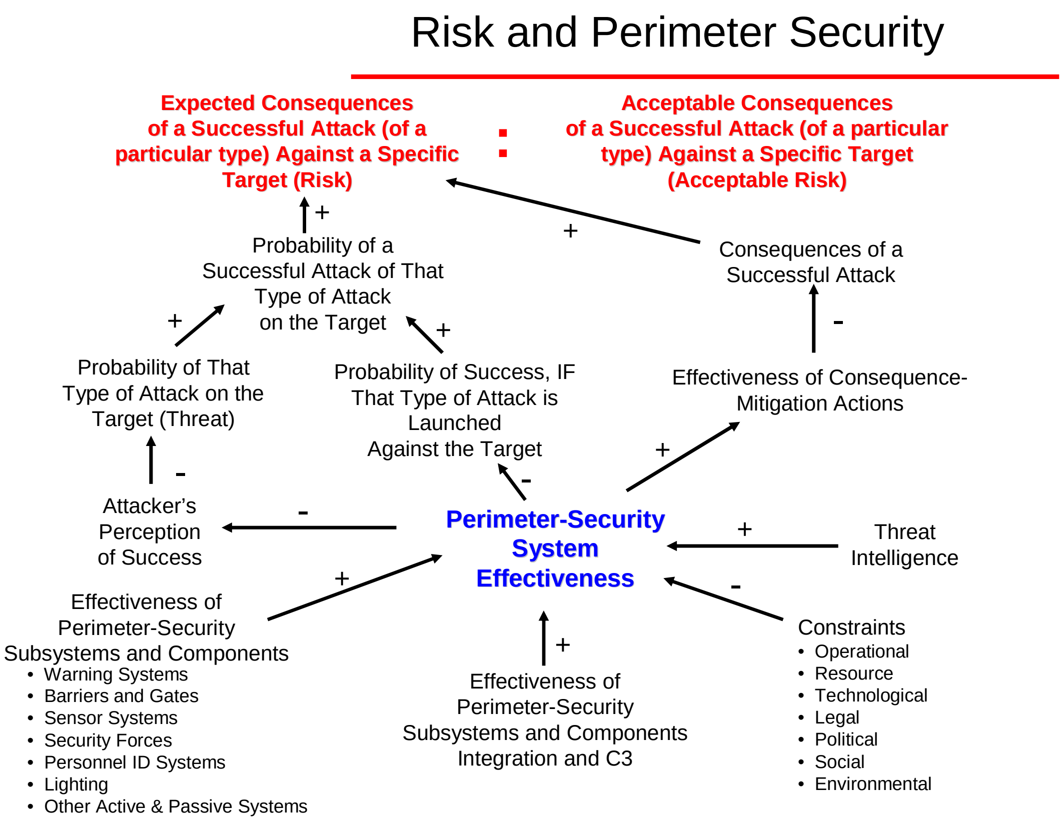

Risk and Perimeter Security
Expected Consequences of a Successful Attack (of a particular type) Against a Specific Target (Risk)
Acceptable Consequences of a Successful Attack (of a particular type) Against a Specific Target (Acceptable Risk)
+
Probability of a Successful Attack of That Type of Attack on the Target
+
Consequences of a Successful Attack
+
+
-
Probability of That Type of Attack on the Target (Threat)
Probability of Success, IF That Type of Attack is Launched Against the Target
Effectiveness of Consequence-Mitigation Actions
-
+
-
Attacker's Perception of Success
-
Perimeter-Security System Effectiveness
+
Threat Intelligence
+
-
Effectiveness of Perimeter-Security Subsystems and Components
• Warning Systems
• Barriers and Gates
• Sensor Systems
• Security Forces
• Personnel ID Systems
• Lighting
• Other Active & Passive Systems
+
Effectiveness of Perimeter-Security Subsystems and Components Integration and C3
Constraints
• Operational
• Resource
• Technological
• Legal
• Political
• Social
• Environmental

Figure 10: Risk and Perimeter Security

- It should be emphasized that the fundamental question in considering the most cost-effective general security strategy and the optimal perimeter-security system within that general strategy is the issue of "acceptable risk," i.e., the acceptable "expected consequences" of a successful attack on the target of interest. Ultimately, this policy decision comes down to a matter of judgment by the responsible individual(s). The model in Figure 10 equates risk to expected consequences, where the consequences can include (e.g.) the dollar-value of damage, the number of casualties, the impact of mission interruption, impact on societal processes and institutions, etc. Clearly, many of these consequences, albeit very real, are difficult to quantify, i.e., the risk may be difficult to quantify. Moreover, individual decision makers vary in their tolerance for risk, with some being risk-averse, others being risk-neutral, and still others having a high risk propensity. As Figure 11 suggests, *all other factors being equal*, the required degree of perimeter-security system effectiveness will be (in general) inversely related to the decision maker's tolerance for risk. However, it should be noted that all other factors are seldom, if ever, equal.

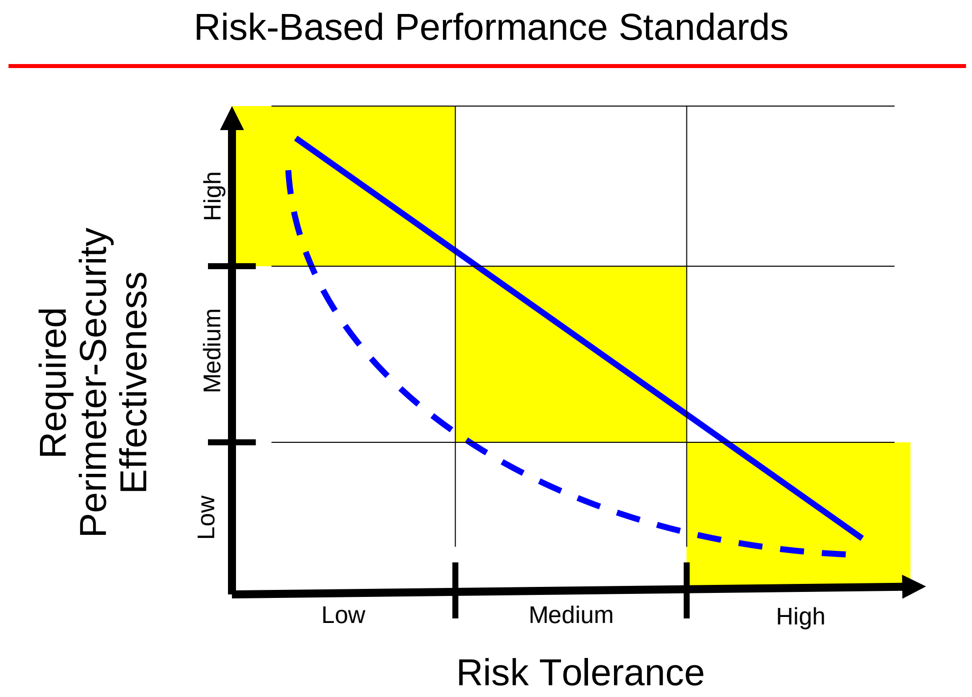


Figure 11: Risk Tolerance and Perimeter-Security Effectiveness

- Ideally, perimeter-security standards should be performance-based, i.e., based on system, subsystem or component functionality – specifying "how well" the system, subsystem or component must perform its intended function. An excellent example of a performance-based system standard is the "Design-Basis Threat" (DBT), used by the U.S. Nuclear Regulatory Commission. The DBT describes the types of threats and attacks on nuclear power plants (and other facilities holding special nuclear materials) that security systems for these facilities must be capable of defeating. The DBT is described in detail in Title 10, Section 73.1(a) of the Code of Federal Regulations ([10 CFR 73.1(a)]. A portion of this DBT can be found in Annex B. This NRC DBT example for nuclear power plants is for illustrative purposes only. The most appropriate DBT (as a perimeter-security system performance standard) for other types of government or non-government facilities or infrastructure will be dependent on a variety of factors, including current intelligence regarding threats and the consequences of a particular type of attack on the specific target.

- The primary focus should be on developing total system performance criteria and associated standards. Subsystem and component criteria/standards are useful, but not as important as specifying how well the total perimeter-security system needs to perform.

- The most important system-performance criterion is effectiveness (sometimes referred to as functionality), i.e., how well the total perimeter-security system accomplishes its intended purpose or function.

- Other criteria for which performance-based perimeter-security system, subsystem and component standards should be considered include:
  - Efficiency
  - Reliability
  - Maintainability
    - Sustainability
    - Flexibility or adaptability
    - Durability
    - Resilience

- Figure 12 attempts to define a general domain for setting standards for perimeter security, considering performance-based criteria, the system as a whole and various subsystems/components, and the risk tolerance of responsible decision makers. The figure highlights that the primary focus should be at the total system level and on system performance effectiveness.

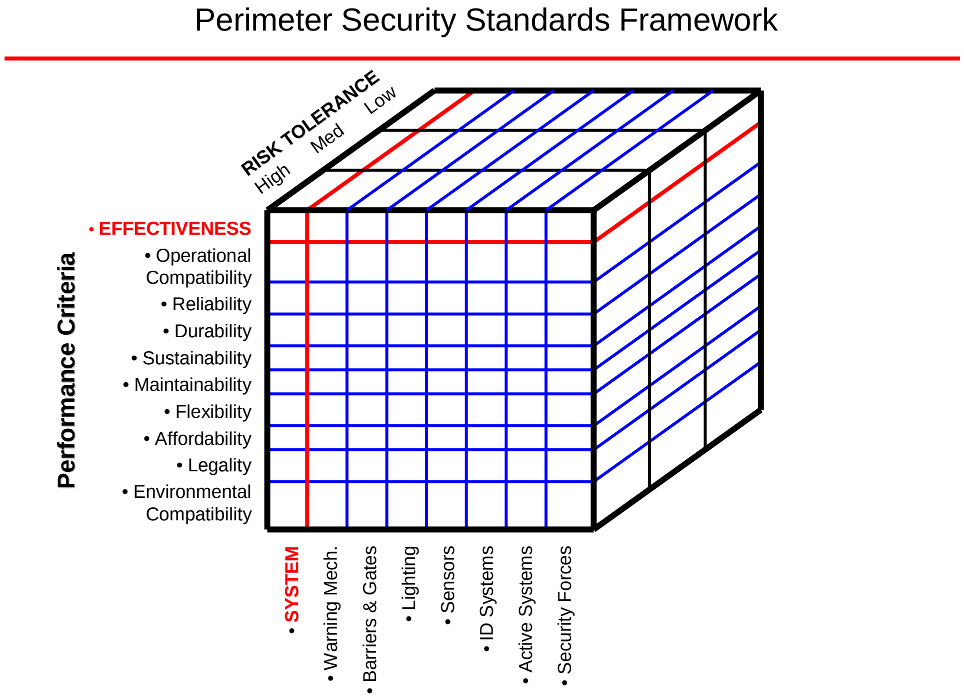


Figure 12: The Domain for Perimeter-Security Standards

- The model illustrated in Figure 12 can also serve as a conceptual framework for systematically considering the need for, and developing, perimeter security standards. For each cell of the matrix, SDOs should do the appropriate "gap analysis:"
  - Do standards exist?
  - Are the existing standards satisfactory, i.e., are they performance based, measurable, etc.?
  - If standards do not exist or existing standards are inadequate or inappropriate, new standards should be considered.

Annex A – Organizations Represented at May 17, 2005 Meeting of the ANSI-HSSP Workshop on Perimeter Security Standardization

American National Standards Institute
American Society of Civil Engineers
Applied Marine Technology, Inc.
ASIS International
Bay Alarm Company
BSI Americas, Inc.
Digital Power Capital
ECSI International, Inc.
EWA Information and Infrastructure Technologies, Inc.
Force Protection Systems Squadron
GE Infrastructure
Hi-Tec Systems
Honeywell Technology Solutions Inc.
Isonics
L-3 Communications, GSI
Lockheed Martin
Mitsubishi Electric Research Laboratories
National Fire Protection Association
ObjectVideo
Professional Systems Engineering, LLC
Raytheon Technical Services Company, LLC
Security Industry Association
Senstar-Stellar Corporation
Telecommunications Industry Association
The JED Group, LLP
The Ohio State University
Trex enterprises
U.S. Army Engineering & Support Center
U.S. Department of Defense
U.S. Department of Homeland Security
U.S. Navy
Underwriters Laboratories
United Nations Development Programme
Washington Group International

Annex B – Excerpt from Design-Basis Threat

DBT is described in detail in Title 10, Section 73.1(a) of the Code of Federal Regulations ([10 CFR 73.1(a)]. A portion of this DBT follows:

General Provisions

§ 73.1 Purpose and scope.

(a) *Purpose*. This part prescribes requirements for the establishment and maintenance of a physical protection system which will have capabilities for the protection of special nuclear material at fixed sites and in transit and of plants in which special nuclear material is used. The following design basis threats, where referenced in ensuing sections of this part, shall be used to design safeguards systems to protect against acts of radiological sabotage and to prevent the theft of special nuclear material. Licensees subject to the provisions of § 72.182, § 72.212, § 73.20, § 73.50, and § 73.60 are exempt from § 73.1(a)(1)(i)(E) and § 73.1(a)(1)(iii).

(1) *Radiological sabotage*.

(i) A determined violent external assault, attack by stealth, or deceptive actions, of several persons with the following attributes, assistance and equipment:

(A) Well-trained (including military training and skills) and dedicated individuals,

(B) inside assistance which may include a knowledgeable individual who attempts to participate in a passive role (e.g., provide information), an active role (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack), or both,

(C) suitable weapons, up to and including hand-held automatic weapons, equipped with silencers and having effective long range accuracy,

(D) hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safeguards system, and

(E) a four-wheel drive land vehicle used for transporting personnel and their hand-carried equipment to the proximity of vital areas, and

(ii) An internal threat of an insider, including an employee (in any position), and

(iii) A four-wheel drive land vehicle bomb.

(2) *Theft or diversion of formula quantities of strategic special nuclear material*.

(i) A determined, violent, external assault, attack by stealth, or deceptive actions by a small group with the following attributes, assistance, and equipment:

(A) Well-trained (including military training and skills) and dedicated individuals;

(B) Inside assistance that may include a knowledgeable individual who attempts to participate in a passive role (e.g., provide information), an active role (e.g., facilitate entrance and exit, disable alarms and communications, participate in violent attack), or both;

(C) Suitable weapons, up to and including hand-held automatic weapons, equipped with silencers and having effective long-range accuracy;

(D) Hand-carried equipment, including incapacitating agents and explosives for use as tools of entry or for otherwise destroying reactor, facility, transporter, or container integrity or features of the safe-guards system;

(E) Land vehicles used for transporting personnel and their hand-carried equipment; and

(F) the ability to operate as two or more teams.

(ii) An individual, including an employee (in any position), and

(iii) A conspiracy between individuals in any position who may have:

(A) Access to and detailed knowledge of nuclear power plants or the facilities referred to in § 73.20(a), or

(B) items that could facilitate theft of special nuclear material (e.g., small tools, substitute material, false documents, etc.), or both.