Argonne NATIONAL LABORATORY

ANL/DIS-13/04

Protective Measures Index and Vulnerability Index: Indicators of Critical Infrastructure Protection and Vulnerability

Decision and Information Sciences Division

ANL/DIS-13/04

Protective Measures Index and Vulnerability Index: Indicators of Critical Infrastructure Protection and Vulnerability

by
F.D. Petit, G.W. Bassett, W.A. Buehring, M.J. Collins, D.C. Dickinson, R.A. Haffenden, A.A. Huttenga, M.S. Klett, J.A. Phillips, S.N. Veselka, K.E. Wallace, R.G. Whitfield, and J.P. Peerenboom
Decision and Information Sciences Division, Argonne National Laboratory

July 2013

Contents

Acknowledgments v
Executive Summary vii
1 Introduction 1
2 Risk, Vulnerability, and Resilience 3
3 Protective Measures Index Methodology 7
3.1 Organization of the Protective Measures Index 10
3.1.1 Physical Security 10
3.1.2 Security Management 11
3.1.3 Security Force 12
3.1.4 Information Sharing 13
3.1.5 Security Activity History/Background 13
3.2 Data Collection 14
3.3 Calculation of the Protective Measures Index 17
3.4 Data Display 20
4 Use of the Protective Measures Index 25
5 Methodology Advantages and Limitations 29
6 Conclusion 33
7 References 35
Appendix A: Protective Measures Index Structure 39
Appendix B: Illustration of Weight Determination 41
Appendix C: Sector and Threat Dependencies of the Weights 47
Appendix D: Example of Calculation Rollup 51
Appendix E: List of Abbreviations 59

Figures

1 Risk Components 3
2 Risk Management Bowtie Diagram 4
3 Level 1 Attributes of the Protective Measures Index 10
4 Levels 2 and 3 Subcomponents of the PMI Contributing to Physical Security 11
5 Levels 2 and 3 Subcomponents of the PMI Contributing to Security Management 12
6 Levels 2 and 3 Subcomponents of the PMI Contributing to Security Force 12
7 Levels 2 and 3 Subcomponents of the PMI Contributing to Information Sharing 13
8 Levels 2 and 3 Subcomponents of the PMI Contributing to Security Activity History/Background 13
9 Overview of the Infrastructure Survey Tool 16
10 Relationship of PMI to VI 19
11 PMI Dashboard Overview Screen 21
12 PMI Dashboard Selections: Physical Security/Fences/Fraction Enclosed 22
13 PMI Dashboard's Brief Review Screen 23
14 Comparison of Resilience and Protective Measures Indices 25
A1 Structure of the Level 1 PMI Components and Subcomponents 39
D1 Relationship of Protective Measures Index to Vulnerability Index 57

Tables

Table B1: Ranks and Relative Importance Defined by SMEs for the Security Plan Exercises Subcomponents 42
Table B2: Notional Relative Importance Obtained for Subcomponents of the Security Plan Exercises 43
Table B3: Notional Weights Obtained for Subcomponents of the Security Plan Exercises 44
Table B4: Notional Weights Obtained for the PMI Level 1 Components 45
Table C1: PSA Physical Security Subcomponent Weights as a Function of Threat 47
Table C2: PSA Physical Security Subcomponent Weights as a Function of Sector 48
Table C3: PSA PMI Component Weights as a Function of Subsector 49
Table D1: Fences Type Index (Illustrative Asset) 51
Table D2: Fences Index (Illustrative Asset) 52
Table D3: Physical Security Index (Illustrative Asset) 53
Table D4: Protective Measures Index (Illustrative Asset) 55

Acknowledgments

The authors gratefully acknowledge the contributions of many people who helped bring this project to its current state of development, and specifically the Protective Security Coordination Division management team of the U.S. Department of Homeland Security Office of Infrastructure Protection.

This page intentionally left blank.

Executive Summary

In 2009, the U.S. Department of Homeland Security (DHS) and its protective security advisors began assessing high-risk critical infrastructure assets using a targeted questionnaire, the Infrastructure Survey Tool (IST), and produced individual vulnerability/protective measure values through the Protective Measures Index (PMI) and Vulnerability Index (VI).

The PMI has been formulated to capture the fundamental aspects of protection for critical infrastructure with respect to all hazards. The PMI methodology generates reproducible results that can support decision-making related to risk management. It complements other indices that have been developed — the Resilience Measurement Index (RMI) and Consequences Measurement Index (CMI) — and thus allows, in combination with other tools, critical infrastructure to be compared in terms of protection, vulnerability, resilience, consequences, and ultimately risk. The main objective of the PMI is to measure the ability of a critical infrastructure system to resist to disruptive events.

The PMI is based on multi-attribute utility theory (MAUT) and decision analysis principles. The Level 1 indices and overall PMI for an asset/facility are based on data collected via the Enhanced Critical Infrastructure Protection Program's IST. The indices are based on the aggregation of pertinent variables in the IST. Each of these variables has been weighted by subject matter experts to indicate their relative importance to a facility's protection. The value of the PMI ranges between 0 (low protection) and 100 (high protection). A high PMI does not mean that a specific event will not affect the facility or have severe consequences. Conversely, a low PMI does not mean that a disruptive event will automatically lead to a failure of the critical infrastructure and to serious consequences. The PMI instead is used to compare the level of protection of critical infrastructure and also guides the prioritization of limited resources for improving protection and lowering vulnerability. The PMI has a constructive aspect in that it improves (values increase) as protective measures are added. The information assists DHS in analyzing sector and subsector vulnerabilities so it can identify potential ways to reduce vulnerabilities and prepare sector risk estimates.

All the data and levels of information used for the PMI, as well as the value of its five Level 1 components, are presented on an interactive, Web-based tool called the IST PMI Dashboard. The PMI dashboard provides a snapshot of the protective measures of a particular critical infrastructure asset at a specific point in time. The IST PMI Dashboard provides valuable information to owners and operators about their facility's status relative to those of similar assets. This comparison provides owners and operators with an indication of which security-related strengths and weaknesses may be contributing factors to its vulnerability and protection posture. The Dashboard can be used to create scenarios and assess the implementation of specific protective measures or procedures that a facility's owners and operators might consider. Using the Dashboard's interactive "Facility Scenario" function makes it possible for an owner or operator to select protection enhancements and immediately see the resulting modified PMI. Policies, procedures, or operational changes are enhancements the facility may implement to increase protection.

Combining the PMI information with other indices, such as the RMI and the CMI, allows analysts to perform a comprehensive assessment of risk that can support decision-making about protection, business continuity, and emergency management of critical infrastructure.

1 Introduction

In 2009, DHS and its protective security advisors (PSAs) began surveying owners and operators of critical infrastructure assets using the Infrastructure Survey Tool (IST). The information collected during visits is used to develop metrics; conduct sector-by-sector vulnerability comparisons; identify security gaps and trends across critical infrastructure sectors and subsectors; establish baseline survey results regarding sector security; and track progress toward improving critical infrastructure security through activities, programs, outreach, and training (Snyder, 2009).

The data generated through this collection effort are used in a framework consistent with the National Infrastructure Protection Plan (NIPP) risk criteria (DHS, 2009). The NIPP framework incorporates consequence, threat, and vulnerability components and addresses all hazards. The analysis of the vulnerability data must be reproducible, support risk analysis, and go beyond protection. It also must address important security/vulnerability topics, such as physical security and systems analysis.

Argonne National Laboratory, in partnership with DHS, developed an index — the Protective Measures Index (PMI) — that identifies the protective measures posture of individual facilities at their "weakest link," allowing for a survey of the most vulnerable aspects of the facilities (Fisher *et al.*, 2009; Petit *et al.*, 2011). The PMI methodology has been developed to estimate protective measures of critical infrastructure sectors and subsectors. In 2010, another index was developed for capturing the resilience of critical infrastructure — the Resilience Index (RI) (Fisher *et al.*, 2010; Petit *et al.*, 2012).

In 2012, Argonne National Laboratory and the U.S. Department of Homeland Security (DHS) Office of Infrastructure Protection enhanced the first version of the RI to better integrate the concepts of business continuity and assessment of dependencies among critical infrastructure assets. This revision has led to a new version of the index — the Resilience Measurement Index (RMI). At the same time, the structure and content of the PMI were reviewed. The objective was to have two complementary indices that do not overlap.

This report provides an overview of the new version of the PMI methodology. The first section explains the relation between vulnerability, risk, and resilience. The second section presents the PMI organizational structure and explains the PMI methodology from data collection to display of results via the IST PMI Dashboard. The third section presents some possible applications for use of the PMI. A fourth section explains the advantages and limitations of the PMI.

This page intentionally left blank.

2 Risk, Vulnerability, and Resilience

DHS defines risk as "*the potential for an unwanted outcome resulting from an incident, event, or occurrence, as determined by its likelihood and the associated consequences*" (DHS, 2010). Risk is thus traditionally defined as a function of three elements: the threats to which an asset is susceptible, the vulnerabilities of the asset to the threat, and the consequences potentially generated by the degradation of the asset (Figure 1).

Figure 1: Risk Components

Threat is a "*natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment, and/or property*" (DHS, 2010). Sometimes the term hazard, which can be defined as a "*natural or man-made source or cause of harm or difficulty*" (DHS, 2010), is used instead of threat. However, as defined by the DHS lexicon, a "hazard differs from a threat in that a threat is directed at an entity, asset, system, network, or geographic area, while a hazard is not directed" (DHS, 2010). Vulnerability is a "*physical feature or operational attribute that renders an entity open to exploitation or susceptible to a given hazard*" (DHS, 2010). Consequences are the "*effects of an event, incident, or occurrence*" (DHS, 2010).

If risk is a function of threats and hazards, vulnerabilities, and consequences, the challenge is to define where and how resilience fits into the determination of risk. Resilience, as defined by DHS, is the "*ability to resist, absorb, recover from or successfully adapt to adversity or a change in conditions*" (DHS, 2010). The DHS lexicon also states that "resilience can be factored into vulnerability and consequence estimates when measuring risk" (DHS, 2010). On the basis of this statement, a facility's resilience would have an effect on both vulnerability and consequences.

Risk management can be defined as the "*process of identifying, analyzing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an*

acceptable cost" (DHS, 2010). Risk management involves knowing the threats and hazards that could potentially impact a given facility, the impacts on the facility because of its vulnerabilities, and the consequences that might result. On the basis of these characteristics, it is possible to develop specific indicators and metrics to assess the risk to an organization. The main objective is thus to analyze the performance of a facility in terms of protection/vulnerability, resilience, consequence, and, ultimately, risk; and to propose options to improve this performance (Figure 2).

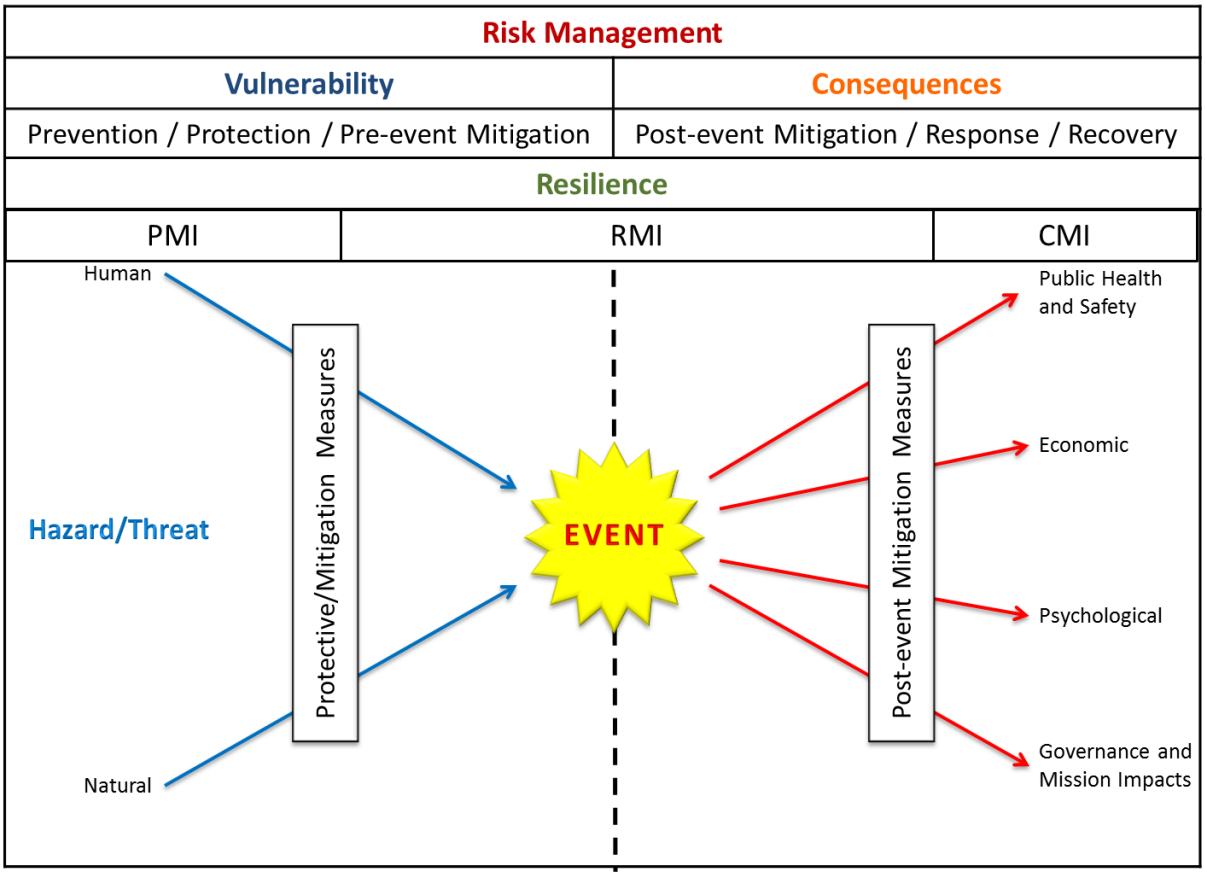


Figure 2: Risk Management Bowtie Diagram

The risk management bowtie presented in Figure 2 represents how threats, vulnerability, consequences, and resilience fit together in a risk management process. Considering a threat or hazard (manmade or natural), the vulnerability and resilience of an organization (and/or infrastructure asset) will impact the potential consequences of an event. The interactions among the components of risk are complex — and are made more so when analysts and owners/operators consider the transfer of risk among assets in the case of a threat by an intelligent adversary. For example, when protection at a site is increased, vulnerability decreases and the risk at that site declines; however, the risk level at another site or sites may increase (Phillips *et al.*, 2012).

The first index developed was the PMI in 2008. This index captures the protective measures in place in a given facility (Fisher *et al.*, 2009; Petit *et al.*, 2011). The objectives of this index were to develop a key performance indicator that allows characterizing the protective posture of a facility and then to support the decisions of critical infrastructure owners and operators by allowing comparison between like facilities. This index needed to be applicable to all types of critical infrastructure sectors/subsectors and also needed to consider all types of hazards. The fourth version of this index, launched in January 2013, addresses elements characterizing physical security, security management, security force, information sharing, and security activity history/background. The PMI focuses on the left side of the risk management bowtie. This index allows users to calculate another indicator: the Vulnerability Index (VI), which is the opposite of the PMI. When the VI is low, the PMI is high, and vice versa. When an owner or operator takes an action that increases an asset's level of protection, the PMI rises and the VI decreases.

The second index, the RMI, characterizes the resilience of critical infrastructure: it is depicted at the center part of the bowtie and mitigates the otherwise maximum consequences depicted on the right side of the bowtie (Fisher *et al.*, 2010; Petit *et al.*, 2012). The second version of this index was launched in January 2013; the RMI addresses elements characterizing preparedness, mitigation measures, response capabilities, and recovery mechanisms (Petit *et al.*, 2013).

A third index, the Consequences Measurement Index (CMI), characterizes the maximum consequences potentially generated by an adverse event at a facility. This index includes information on public health and safety, economic, psychological, and governance and mission impacts from the loss of the facility. This index focuses on the right side of the risk management bowtie.

Section 3 presents the methodology used for developing the PMI and the VI.

This page intentionally left blank.

3 Protective Measures Index Methodology

In its continued effort to secure the United States' critical infrastructure, DHS developed the Enhanced Critical Infrastructure Protection (ECIP) Program, which aims to increase communication between DHS and critical infrastructure owners/operators, and collect information about facilities' current protective measures and overall security posture.

As part of identifying the current protective measures and security postures of facilities, the ECIP Program attempts to analyze the vulnerability of specific facilities and thus build, in aggregate, a picture of vulnerability for entire infrastructure sectors. This focus on vulnerability as a component of risk — and thus a necessary element in planning for and executing strategies to enhance critical infrastructure protection — falls in line with a risk-based approach emphasized by DHS and called for by the U.S. Government Accountability Office (2007, 2008a, 2008b). However, properly instituting a risk-based approach to prioritizing and carrying out protective measures for critical infrastructure requires that the components of risk — threat, criticality, and (in the case of ECIP) vulnerability — must be properly and consistently understood (DHS, 2009).

The term *vulnerability* is used in many contexts, including in engineering, finance, environmental studies, and, in this case, homeland security. At its most basic definition, vulnerability captures the susceptibility of a person, system, asset, or environment to a specific threat scenario (Ezell, 2007). The scenario (an attack, structural failure, or a damage event) is often negative in nature. For use in critical infrastructure protection, the scenario often revolves around susceptibility to a successful attack or damage event (whether purposeful or not, human caused or naturally occurring). The ambiguous nature of the words "attack" or "damage event" often relegates attempts to assess vulnerability to being either "too narrow" for common application or "too broad" from which to draw sound conclusions.

Some methodologies tend to capture threat probability as part of the vulnerability assessment, whereas others incorporate probability in a separate threat component and not as a distinct portion of the vulnerability component. Because probability is an important aspect of calculating overall risk, it should be captured somewhere in an overall risk methodology; however, it may be appropriate to analyze it both as part of a vulnerability assessment or as a separate piece in the equation.[1]

Types of vulnerabilities vary according to the nature of the threat. The vulnerability can be static if it is relatively insensitive to the nature of the threat (e.g., lack of a security management plan). It can also be dynamic if its characteristics vary based on the nature of the threat (e.g., fence type). Furthermore, the vulnerability analysis will depend on the way the threat is taken into account. Indeed, it is possible to consider the vulnerability of a particular asset to a particular threat or to consider multiple potential specific sequences of events.

[1] We distinguish probability related to a successful event or occurrence from uncertainty here. The uncertainty in the vulnerability factor could also be represented as a probability.

Regardless of the configuration of vulnerability methodologies, in order to develop a methodology that is usable for the greater critical infrastructure community and produces appropriate results, four main functional requirements must be met:

1. The vulnerability methodology must be usable in all 16 of the DHS critical infrastructure sectors, yet also have the ability to be tailored to the specific operational needs of individual sectors/subsectors.

   In order to benefit the critical infrastructure community at large, a vulnerability methodology must be able to assess and compare vulnerability within sectors, between facilities, and across the full spectrum of critical infrastructure to understand the sectors' and subsectors' current security postures and susceptibility to threats, as well as to prioritize national protection efforts based upon the results. At the same time, the methodology needs to be flexible enough so that it can be tailored to specific sectors and thus capture the most appropriate picture of vulnerability. This flexibility must still maintain the external validity of the methodology to enable comparisons.

2. The methodology must be adaptable to a range of threat scenarios because vulnerability will differ depending on the scenario analyzed.

   An infrastructure asset's level of vulnerability is dependent upon the scenario applied against a facility. Therefore, in order to assess a range of threat scenarios, the methodology must be constructed with a "built-in" ability to adapt based upon different scenarios. Although the methodology might not differ significantly between a threat scenario involving a person-carried improvised explosive device (IED) and a vehicle-borne IED, the results would be expected to vary significantly between an IED threat scenario and a cyber-attack scenario.

3. The methodology must yield reproducible results by reducing subjectivity and ambiguity.

   Many current methodologies require users to estimate vulnerability components on subjective scales (e.g., with "5" representing a highly protected perimeter and "1" representing a perimeter not protected at all). These subjective elements lead to a lack of reproducibility as values may depend more upon the person utilizing the tool than the actual state of the facility. Reducing these areas of subjectivity by asking basic factual questions (e.g., "is the facility surrounded by a fence?") greatly reduces subjectivity.

4. The methodology must produce results that benefit owners, operators, and coordinating/oversight entities, such as DHS.

   To encourage owners and operators to make use — apart from regulatory mandates — of a vulnerability methodology, said methodologies should produce results that owners and operators find to be of benefit. In addition, all results and products resulting from the methodology must be beneficial to the sector's coordinating and oversight bodies. The results or products of the methodology must also explain to owners and operators what the resulting information means and how it can help them in day-to-day operations, as well as in strategic planning.

Considering the above requirements, this report proposes a vulnerability methodology for use by DHS. The methodology can be used within all critical infrastructure sectors and is part of a larger risk methodology.

The PMI structures the information collected in five categories — namely, Physical Security, Security Management, Security Force, Information Sharing, and Security Activity History/Background —to characterize the protective posture of an entity.

The PMI calculation is based on information collected using the IST. The IST questions were developed on the basis of security and risk management standards and manuals and especially draw from the following:

- FEMA 426 – Risk Management Series – Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings (FEMA, 2003);

- FEMA 452 – Risk Management Series – Risk Assessment: A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings (FEMA, 2005);

- ASIS – Protection of Assets Manuals (ASIS, 2012); and

- Physical Security Criteria for Federal Facilities – An Interagency Security Committee Standard (Interagency Security Committee, 2010).

Appendix A presents a flow chart of the PMI structure. The organization and the different elements constituting the PMI are discussed in the following sections.

3.1 Organization of the Protective Measures Index

Based on security standards and manuals (e.g., FEMA 426, FEMA 452, and ASIS Protection of Assets Manuals), the PMI combines the information collected in five categories, which are also called PMI Level 1 components (Figure 3).

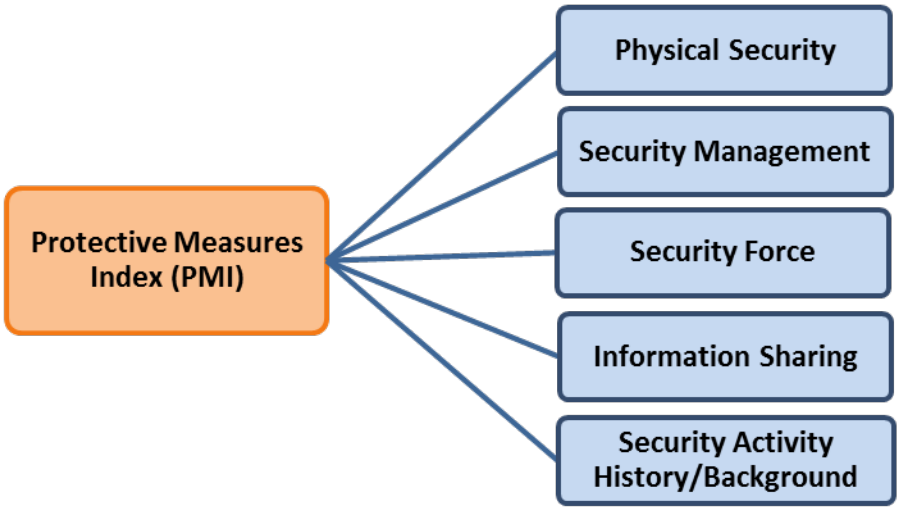


Figure 3: Level 1 Components of the Protective Measures Index

The PMI organizes the information collected with the IST into four levels of information in order of increasing specificity; raw data are gathered at Level 4. These are then combined further through Levels 3, 2, and, finally to Level 1. Each of the Level 1 components is defined by the aggregation of Level 2 subcomponents that allow analysts to characterize a facility. The PMI is constituted by five Level 1 components, 25 Level 2 subcomponents, and 64 Level 3 subcomponents, as defined by subject matter experts (SMEs).

The following sections present the definition and overview of each Level 1 components and associated Level 2 subcomponents that contribute to the PMI calculation.

3.1.1 Physical Security

Physical Security refers to measures and features that protect a facility and its buildings, perimeter, and occupants from intrusion. In the PMI, Physical Security is subdivided into nine Level 2 and 31 Level 3 subcomponents (Figure 4).

The Physical Security component is influenced by the presence or absence of fences, gates, barriers, electronic surveillance (e.g., closed-circuit television and intrusion detection system), parking controls, illumination, entry control procedures, and building envelope (e.g., windows, doors, walls, ceiling/roof, air handling, and facility access), and their characteristics (e.g., for fences, Physical Security integrates their type, height, base, and the fraction enclosed).

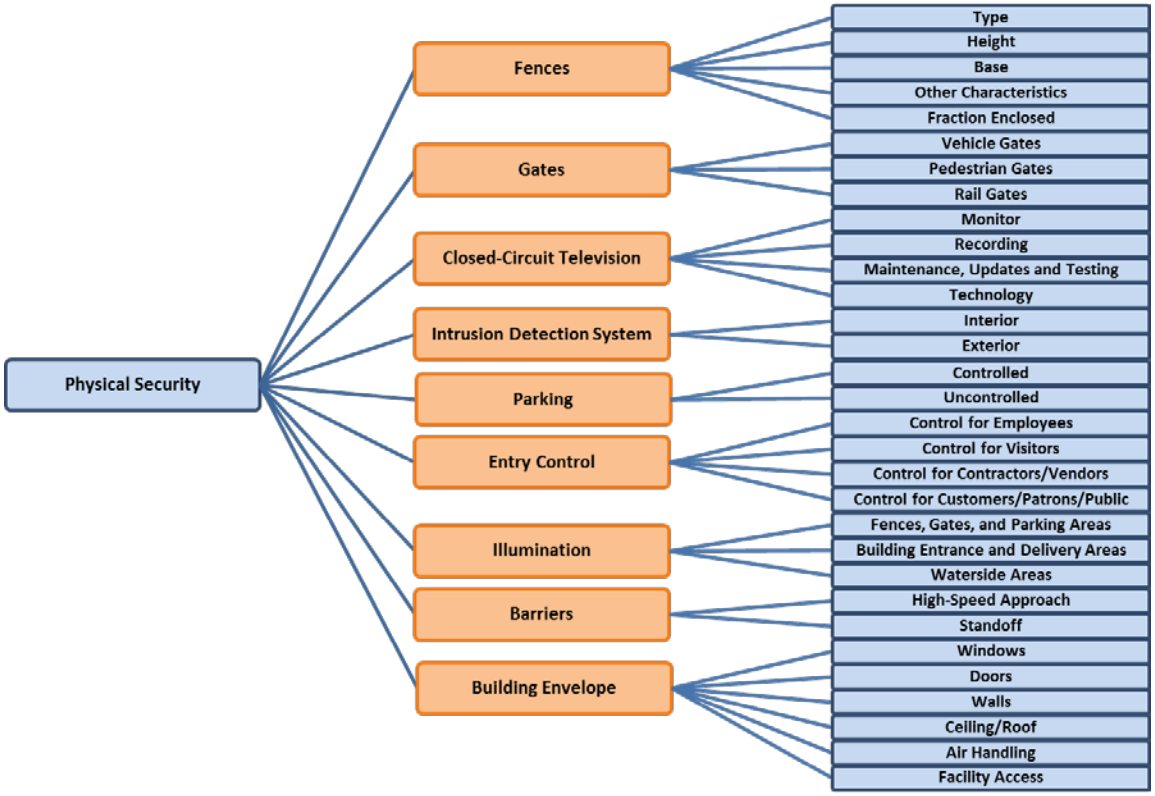


Figure 4: Levels 2 and 3 Subcomponents of the PMI Contributing to Physical Security

3.1.2 Security Management

Security Management refers to plans and procedures a facility has in place to deal with security issues. In the PMI, Security Management is subdivided into seven Level 2 and six Level 3 subcomponents (Figure 5).

The presence or absence of a security manager, security plans and communications, procedures for handling suspicious packages and sensitive information, interactions with security working groups, and background checks influence the Security Management subcomponent.

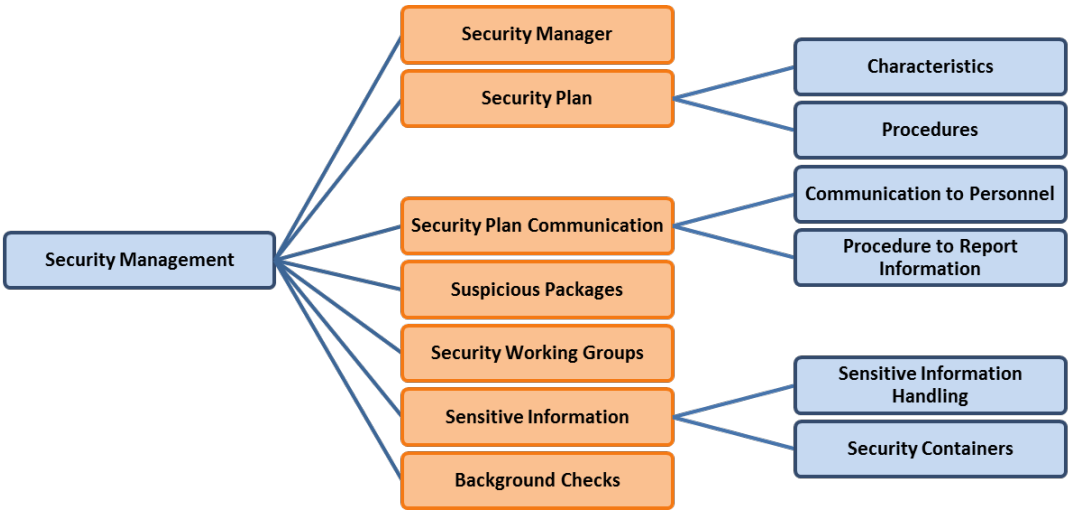


Figure 5: Levels 2 and 3 Subcomponents of the PMI Contributing to Security Management

3.1.3 Security Force

Security Force refers to a special group of employees or contractors with security duties. In the PMI, Security Force is subdivided into five Level 2 and 15 Level 3 subcomponents (Figure 6).

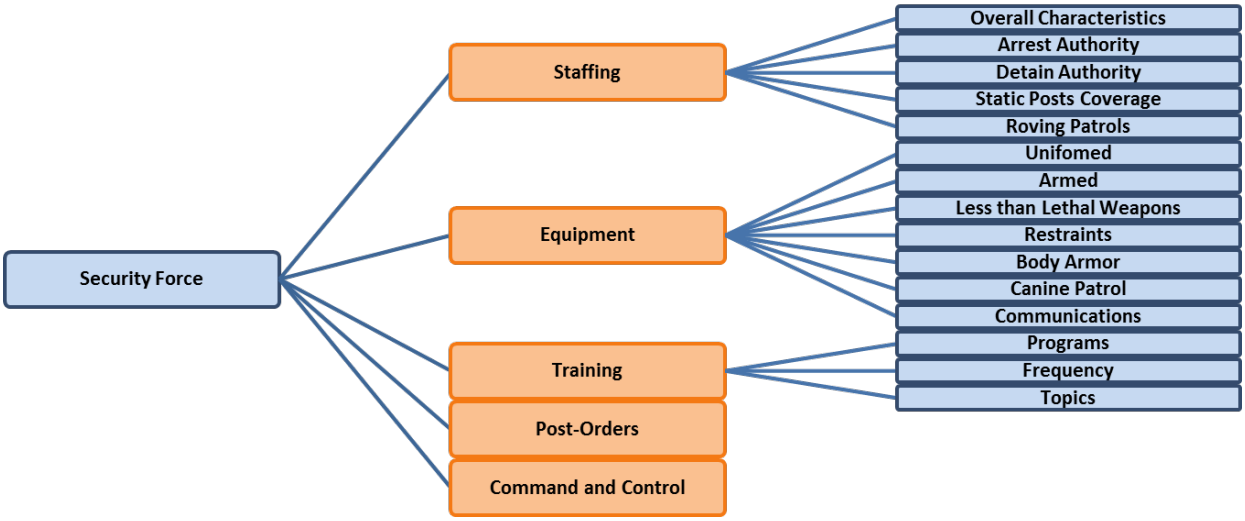


Figure 6: Levels 2 and 3 Subcomponents of the PMI Contributing to Security Force

The presence or absence of staffing, equipment, training, post orders, and a command-and-control center influences the Security Force subcomponent. Training subcomponent combines information characterizing the types of programs, the training frequency, and the different topics (e.g., emergency response, facility-specific standard operating procedures, weapons and self-defense, and screening and access) addressed during the training.

3.1.4 Information Sharing

Information Sharing refers to the exchange of hazard and threat information with local, State, and Federal agencies. In the PMI, Information Sharing is subdivided into two Level 2 and two Level 3 subcomponents (Figure 7).

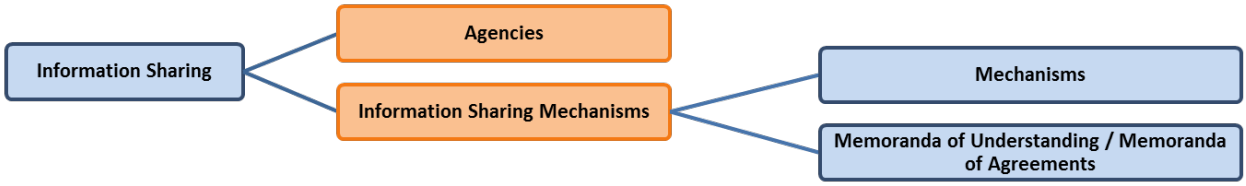


Figure 7: Levels 2 and 3 Subcomponents of the PMI Contributing to Information Sharing

The presence or absence of threat sources, employees with a national security clearance, coordination of security plans with local law enforcement, participation in security working groups, and written memorandums of understanding (MOUs) and memorandums of agreement (MOAs) with agencies and personnel other than emergency responders influence the Information Sharing subcomponent.

3.1.5 Security Activity History/Background

Security Activity History/Background collects information related to previous vulnerability assessments and new protective measures that a facility may have implemented within the last year to improve its security posture. In the PMI, Information Sharing is subdivided into two Level 2 and ten Level 3 subcomponents (Figure 8).

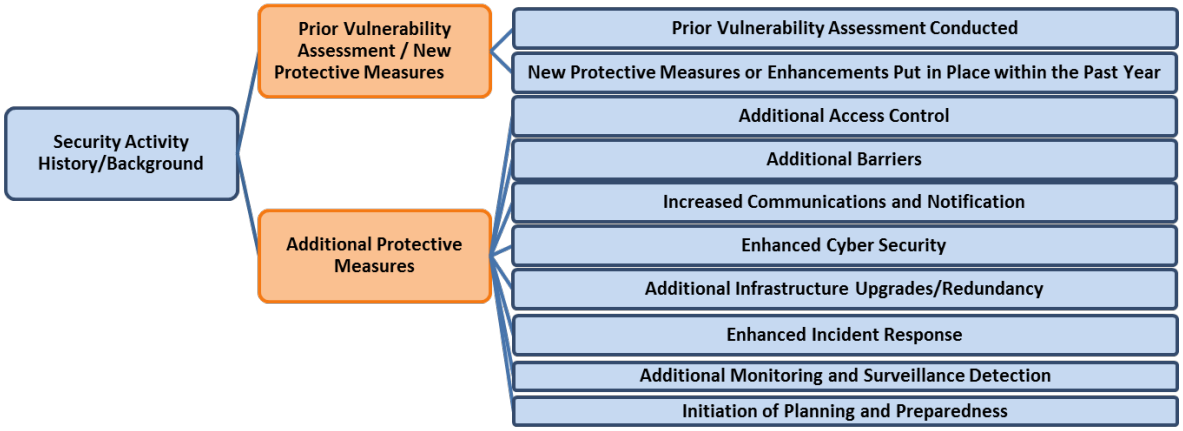


Figure 8: Levels 2 and 3 Subcomponents of the PMI Contributing to Security Activity History/Background

The presence or absence of prior vulnerability assessments, new and additional protective measures, different threat levels in security plans, and additional protective measures during elevated threat situations influence the Security Activity History/Background subcomponent.

3.2 Data Collection

The main objective for calculating the PMI is to capture the performance of an organization in terms of protection/vulnerability. To do so, it is necessary to obtain quality data that can be analyzed in the model.

The DHS ECIP program, IST, and Site Assistance Visits (SAVs) utilize surveys to gather data on the protective and resilience performance of critical infrastructure assets/facilities (DHS, 2013a, 2013b). A visit is usually conducted in four hours to two days, depending on the complexity and size of the facility. During this time, the assessors, who are either PSAs or a specially trained National Guard (NG) team, meet with key facility personnel (e.g., security manager, operations manager, utilities manager, and cyber security manager) and ask them to characterize their protective posture and continuity activities, based on the questions in the IST. The local PSA is tasked with establishing contact with a facility's owners and operators and providing insights into DHS activities and programs to the facility. All of these survey programs are voluntary. The facility owner or operator specifies if they would like DHS to protect the information provided via the Protected Critical Infrastructure Information (PCII) program.[2] It is important to note that the ECIP and SAV collection processes are not related to regulatory efforts. For the PMI, the information collected characterizes the weakest protective measures (i.e., the weakest portion of fence if types and characteristics vary). The information needed for the PMI calculation, as set forth in the preceding sections, is collected using the secure online IST (Figure 9).

The IST is organized in 23 sections that allow the assessor to collect pertinent information which characterizes the protection, resilience, and consequences at a specific facility. This tool allows the assessor to capture general information about the site visited and to highlight commendable activities and measures, as well as identify vulnerabilities and provide options for consideration to improve the facility's protection and resilience posture.[3]

Information from the following eleven (11) of the 23 sections defined in the IST are used in the PMI calculation:

1. Information Sharing;
2. Security Activity History/Background;
3. Security Management Profile;

[2] Information provided during an ECIP assessment may be protected under the Protected Critical Infrastructure Information Act and its implementing regulations. See 6 Code of Federal Regulations Section 29, available at http://www.gpo.gov/fdsys/pkg/CFR-2013-title6-vol1/xml/CFR-2013-title6-vol1-part29.xml, accessed July 15, 2013.

[3] In its 23 sections, the IST captures information for the Protective Measures Index, the Resilience Measurement Index, and the Consequences Measurement Index.

4. Security Force Profile;
5. Perimeter Security;
6. Entry Controls;
7. Parking/Delivery/Standoff;
8. Barriers;
9. Building Envelope;
10. Electronic Security Systems; and
11. Illumination.

Three main elements allow users to ensure the uniformity and reproducibility of the data collected:

1. Helps and explanations;
2. Training; and
3. Quality Assurance (QA) review.

The IST Helps and explanations provide a detailed description for each question and what it is intended to capture.

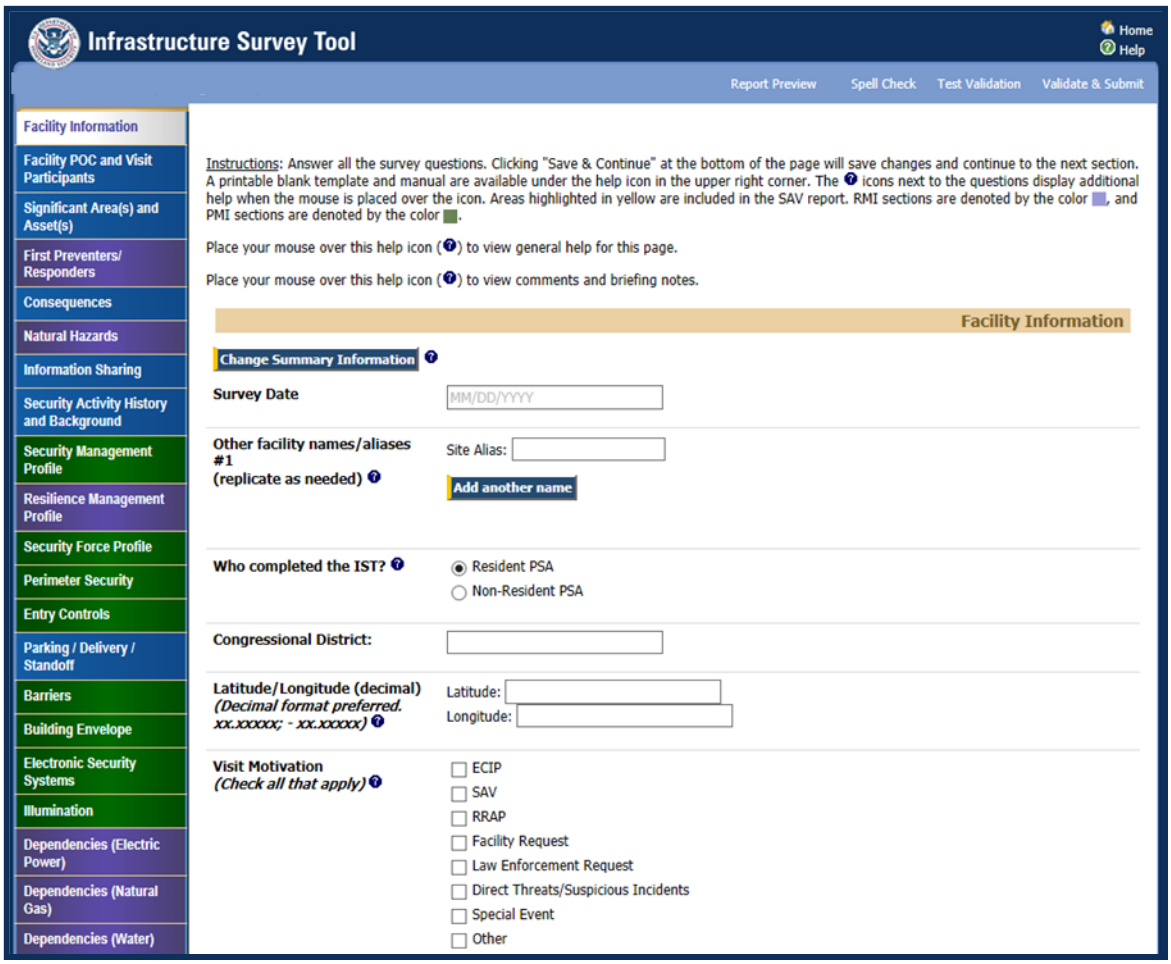


Figure 9: Overview of the Infrastructure Survey Tool (IST)

PSAs and NG teams are trained not only on how to conduct the visits, including interviews with the critical infrastructure owners and operators, but also on how to understand the intent of the different questions and how they are used to calculate the indices. Information used for the PMI is collected for the most vulnerable point (weakest fence, entry control, etc.). Questions used for the RMI capture the elements in place that contribute to the resilience of the facility. Finally, the information contributing to the CMI is collected for the worst case scenario (i.e., the consequences generated by the loss of the facility).

The data collected are then verified at both DHS headquarters and Argonne National Laboratory through a QA review process that comprises six steps:

1. The information is "validated" for completeness upon initial submission. An assessor cannot submit the data about a particular facility until all required questions are answered.

2. An initial QA review is conducted by specially trained DHS or NG analysts who have direct and immediate access to the questionnaire to ensure that data collected matches IST methodology and highlight data inconsistencies.

3. A second QA review is conducted by DHS or NG analysts. This second review provides for an objective assessment of the initial QA, including refinement of the process in case the methodology was not followed appropriately. The analysts approve or disapprove changes made during the initial QA review.

4. The PSA then reviews the revised data to approve the changes, to further clarify the information that will become part of the dashboard and/or assessment report, and to help maintain consistency in the methodology.

5. After the PSA review, a final QA review is conducted by another round of SMEs. This final review serves to ensure that data collected matches IST methodology and finalize data QA entries into the database for dashboard development.

6. A final check is conducted during the development of the PMI (scoring process) from the raw data to help ensure that all of the selected elements are properly reflected in the database.

The training, "Helps," and QA processes are an integral part of the larger methodology because they maintain the reproducibility of the information collected and the products disseminated. In addition, verifying the data before producing the index reduces the overall time it takes to return a final product to a facility's owners and operators.

Beyond its benefits for the end product, the QA process also has several other benefits. The PSA and NG reviews serve as continual training opportunities that reinforce, over time, a consistent application of the methodology. The QA process can also highlight problems that may exist in

the question set. The questions and their potential responses can be reevaluated following identification of a pattern of errors. Often, questions or Helps are revised to enhance their clarity and promote consistency of interpretation.

After the QA review process, the data are stored in an Oracle database, allowing not only for management and selection of the data that will be used to calculate the different indices (PMI, RMI, and CMI). The database can be accessed for specific studies and to calculate metrics that evaluate the capabilities of critical infrastructure in terms of vulnerabilities and resilience.

3.3 Calculation of the Protective Measures Index

The PMI is based on decision analysis and MAUT. Each attribute contributing to the facility protection is decomposed into its individual subcomponents, which are then organized into four levels of information. The PMI is defined by the aggregation (roll-up) of multiple data elements which characterize the components and subcomponents.

Argonne National Laboratory has worked in partnership with DHS and its predecessors over the past ten years to develop a comprehensive methodology based on the principles of "decision analysis," an approach that can be used to manage risk under conditions of uncertainty (Keeney, 1992; Keeney and Raiffa, 1976). The methodology uses a numerical representation of a value pattern by comparing different elements of a facility and by using the relations "better than" and "equal in value to" to define their relative importance. Another important element in this decision analysis tool is the transitivity of the ranking. This approach produces a relational representation of a facility's protection alternatives by providing a numerical value assignment for each of its subcomponents.

This methodology characterizes a facility with respect to its subcomponent properties (e.g., content of the security plan; presence of security force), which results in possible decisions and proposals for different alternatives or measures to increase protection. This method helps decision makers to make choices in the context of a seemingly complex issue.

A relative weight is assigned for each characteristic that contributes to the overall protection of the facility. The weights for a set of subcomponents depend on the ranges (worst to best) that are included as options in the question set. Preferences for the specific values within the ranges of single subcomponents and relative weights have been determined based on input provided by SMEs and sector/subsector representatives via a formal elicitation process. Each SME was asked to define the relative importance of each subcomponent compared to other subcomponents at the same level, from the raw data level to the Level 1 components. The process of assigning weights is best explained by considering a specific case. As illustrated in Figure 3, the PMI comprises five Level 1 components: Physical Security, Security Management, Security Force, Information Sharing, and Security Activity History/Background. Considering these five components, the most important[4] component is assigned a rank of 1, the next most important is assigned a rank of 2, and so on. Next, the component ranked first is assigned a value of 100. The component ranked

[4] Given that all things that comprise each Level 1 component are at their best (i.e., most effective) levels, the most important Level 1 component is the one that makes the greatest contribution to protection.

second is assigned a value less than or equal to 100, based on its relative importance in comparison to the component assigned a rank of 1. This process is repeated until a value between 0 and 100 is assigned to each Level 1 component. This logic applies to all levels. Once the SMEs defined the ranks and relative values for a given set of information, a period of discussion allowed them to exchange and explain the elements that guided their thinking. On the basis of this discussion, the SMEs could revise the ranks and relative values. A global relative value is defined for each component based on the SMEs revised values. The same exercise was repeated for each subcomponent in the PMI. Thus, each type of data collected and each element comprising Levels 4 through 1 has been weighted by the SMEs, mostly PSAs, to represent the relative importance of components and subcomponents compared with other data in the same groupings, considering their contribution to the overall protection of a critical infrastructure. Conditions suitable to linear additive functions are assumed to hold for all PMI calculations. Sensitivity analysis to date indicates that this assumption is reasonable. An illustration of the process for determining the weights is presented in Appendix B.

Level 1 and Level 2 weights were obtained for several sectors and subsectors over several relevant threat categories. Each sector assessment includes specification of appropriate subsectors[5] and most relevant threat categories for that sector. Sectors typically include two to six subsectors and up to six threats. In all cases, weights were obtained for general, improvised explosive device (IED), and vehicle-borne improvised explosive device (VBIED) threats. Sector representatives could specify additional threats deemed relevant either for the sector as a whole or for specific subsectors. An example of weights obtained for different sectors and type of threats is presented in Appendix C.

The preferred evaluators for determining Level 1 and Level 2 weights are security experts that represent the owners and operators of the critical assets. Until such judgments have been obtained, representative sector groups are used. To establish that the set of weights obtained from the PSA group is reasonable; judgments about all level of weights were obtained over several days with senior security managers who belong to a Chicago-area professional society. Those results demonstrated general agreement with the weights obtained from the PSAs.

The PMI is defined by the aggregation of four levels of information. For each subcomponent, an index corresponding to the weighted sum of its subcomponents is calculated. This process results in an overall PMI that ranges from 0 (low protection) to 100 (high protection) for the critical infrastructure analyzed, as well as an index value for each Level 1 through Level 3 subcomponent.

The PMI enables users to determine a vulnerability index (VI), which corresponds to the reverse case of the PMI. Figure 10 shows the relationship between the VI and the PMI. When the PMI is low, the VI is high, and vice versa.

[5] The number of appropriate subsectors for this evaluation of vulnerability depends on the differences in security postures within the sector rather than on the number of official subsectors that exist in the DHS sector taxonomy. For example, the Transportation System Sector has identified three subsectors or groups based on security posture: public access nodes (e.g., rail stations), controlled nodes (e.g., control centers), and segments (e.g., open track).

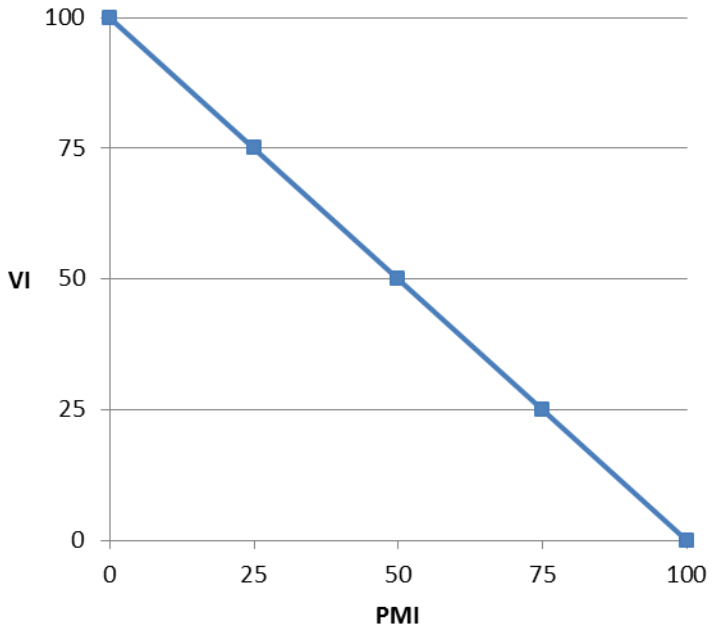


Figure 10: Relationship of PMI to VI

The VI ranges from 0 (low vulnerability) to 100 (high vulnerability). This index is intended to provide a summary value indicating a facility's vulnerability based on data in the IST. It is important to note that a VI of 0 does not mean that the facility is not vulnerable. Rather, the VI represents the combination of all protective measures, procedures, and policies identified within the IST that result in the lowest vulnerability. Thus, the VI is related to, but does not correspond precisely with, the probability of success of an attack, which is sometimes thought of as vulnerability.

This method for characterizing the protection and vulnerability of a critical infrastructure allows DHS to consider the specificity of all subsectors but also to compare the efficiency of different measures to enhance protection in the studied system. An example of the calculation process is presented in Appendix D.

The value of the PMI is 0 (VI is 100) if the facility does not have any of the elements that contribute to the index, and 100 (VI is 0) if the facility has implemented the best option for all the elements contributing to the PMI. The PMI is an indicator of the degree to which the important elements contributing to protection (e.g., security management plan, physical security) have been implemented by a given facility. A value of 0 does not mean that the facility has no protective features or that every type of threat will lead to its immediate shutdown. A facility may have a very low PMI but may also have no reason to increase its PMI because there is no or very little crime in its vicinity, no history of credible threat against the facility, or relatively insignificant consequence(s) if the facility were attacked. In addition, the IST does not collect all information about a facility, just information on the weakest links. Therefore, some other characteristics of a facility could easily override these vulnerability elements. The IST and its associated indices (PMI and VI) are not a vulnerability assessment or a risk assessment. The IST is a basic data collection tool most similar to a security survey. However, if the groupings for

asset comparisons are selected appropriately, PMI and VI comparisons among assets may be informative and may help in identifying areas for more in-depth analysis of potential improvements. On the other hand, a PMI of 100 does not mean that the facility is protected against all types of threats. Thus, a PMI score of 50 can be interpreted as meaning that the protective value/worth of elements, present at the facility, contribute protective features that, in total, amount to half of the maximum PMI. However, a value of 50 does not mean that 50 percent of the elements considered in the PMI calculation are in place at the facility. Indeed, a PMI of 50 can be obtained in different ways by combining different subcomponents of protection. If the value of the PMI increases, the protective capabilities of the facility in one or more of the Level 1 areas (i.e., physical security, security management, security force, information sharing, and security activity history/background) are improved.

It is important to note that the PMI is a relative measure. A high PMI (and low VI) does not mean that a specific event will have minimal consequences. Simply stated, the PMI index allows comparison of different levels of protection of critical infrastructure. The scaling of the index[6] is such that an improvement from 20 to 40 is equivalent to improvement from 60 to 80. Determining a facility's PMI and how different options affect PMI can be used to assess the relative benefits from a variety of options to improve a facility's level of protection.

3.4 Data Display

The comparison of a facility's PMI value to that of other like facilities allows for an appropriate analysis of a facility's protection and has a role in facility risk management.

While important in terms of the data it represents, without a frame of reference, the value generated by the index does not convey its full meaning. For instance, without a frame of reference for similar types of facilities, does an overall PMI value of 55 lead one to believe the facility is quite protected? Or possibly lacking key protective measures? Indeed, this value is strongly related to a specific type of sector and to the context of a facility's operating environment.

An individual index value becomes meaningful when compared with the index values of a set of similar facilities. Providing a facility's owners and operators with a detailed analysis of its PMI and a comparison across other similar facilities is useful because it provides perspective about how the facility's protective measures compare to its peer group.

All the data and levels of information used for the calculation of the PMI, as well as the value of the PMI and of its five level 1 components, are presented on an interactive, Web-based tool called the IST PMI Dashboard. At the top of the Dashboard screen, different tabs allow users to select, from an Overview, one of the five Level 1 PMI components (Physical Security, Security Management, Security Force, Information Sharing, and Security Activity Background) or a Brief Review. Figure 11 shows an example of the Overview Screen.

[6] As determined from elicitations of protective measures experts.

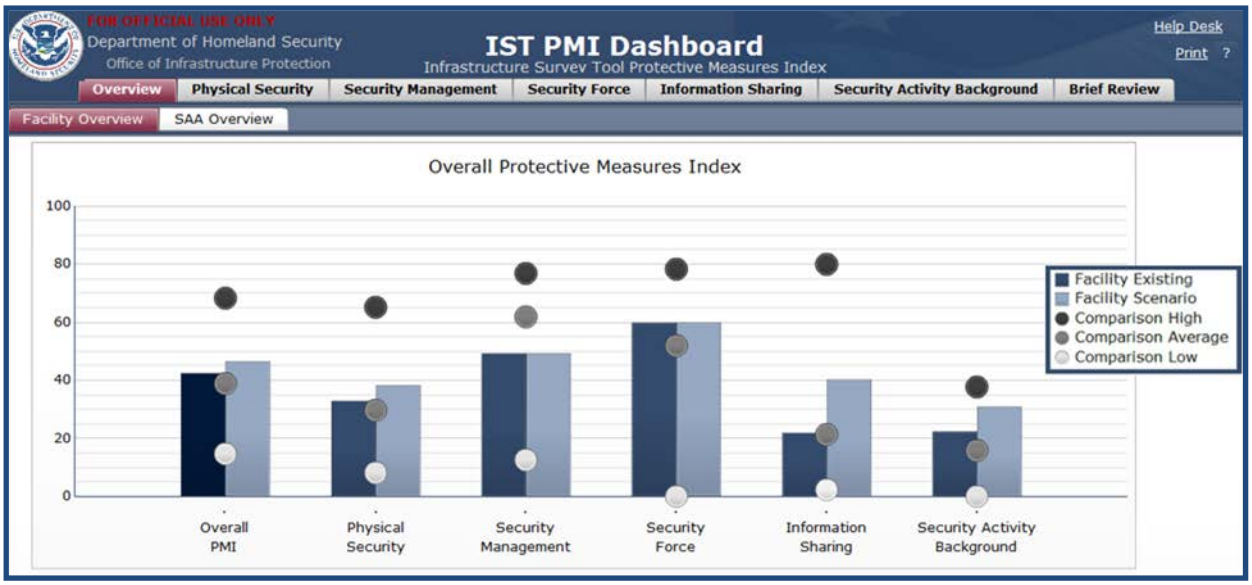


Figure 11: PMI Dashboard Overview Screen (Illustrative Asset)

The Overview Screen shows six dark blue bars representing the existing values for the assessed facility, and six light blue bars, which will change from the existing values to scenario values on the basis of changes input by the user. The bars on the Overview Screen are for overall PMI and the five Level 1 components of the PMI (Physical Security, Security Management, Security Force, Information Sharing, and Security Activity Background). Furthermore, the set of three dots provides a comparison of the facility to other facilities in the same comparison group (e.g., sector, subsector, or segment). The dots display the low, average, and high index values for facilities that have been previously assessed within a similar taxonomy grouping.

The dashboard is an interactive tool in that users can change the characteristics of the subcomponents contributing to the PMI and then compare a scenario value to the existing value, which was determined based on information gathered during the visit, to see whether a potential change can improve the overall PMI of a facility. The user can change an option/characteristic at any of the levels by selecting the corresponding tab in the dashboard. The characteristics of the facility corresponding to the selection made with the drop-down menus appear in the middle of the screen. The user can choose different characteristics and thus create the scenario he or she wants to test. At the bottom of the screen, the user can see — in real time — the impacts of subcomponent modifications on the overall PMI value, as well as on the subcomponents selected with the drop-down menus (Figure 12).

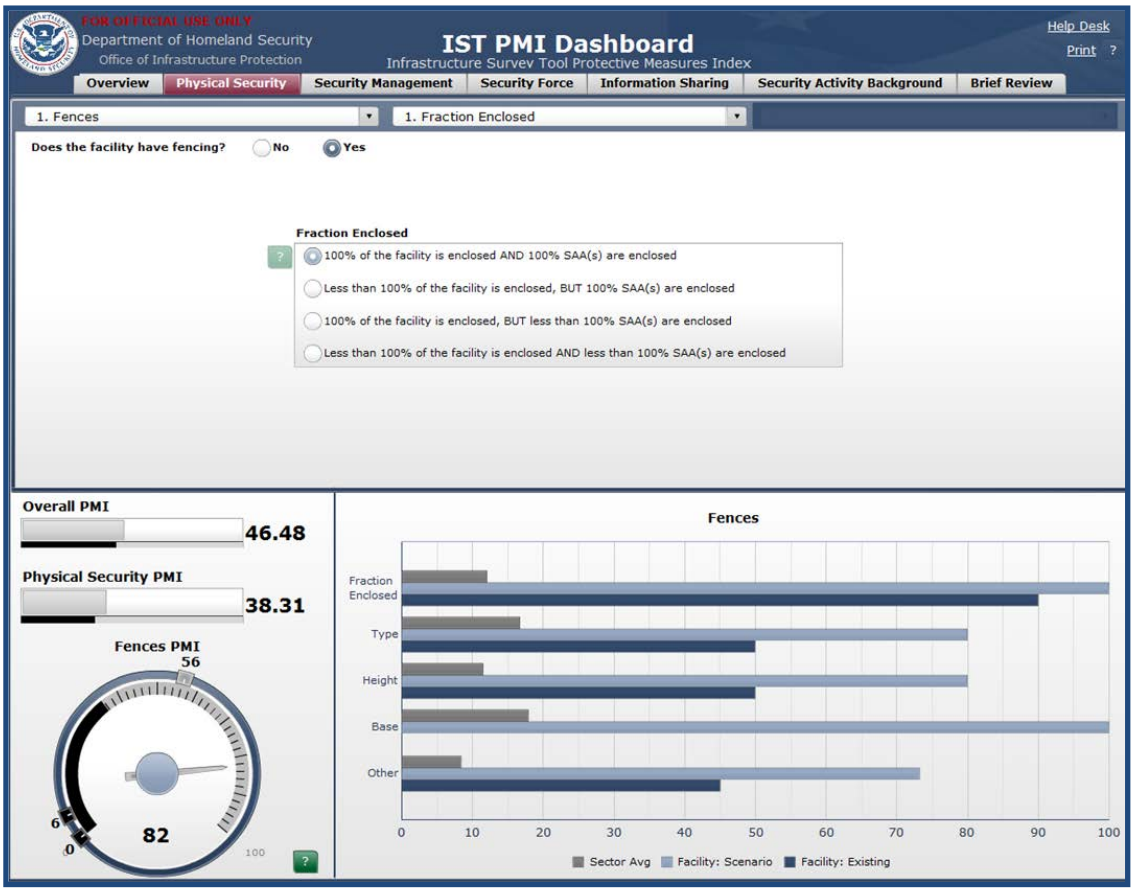
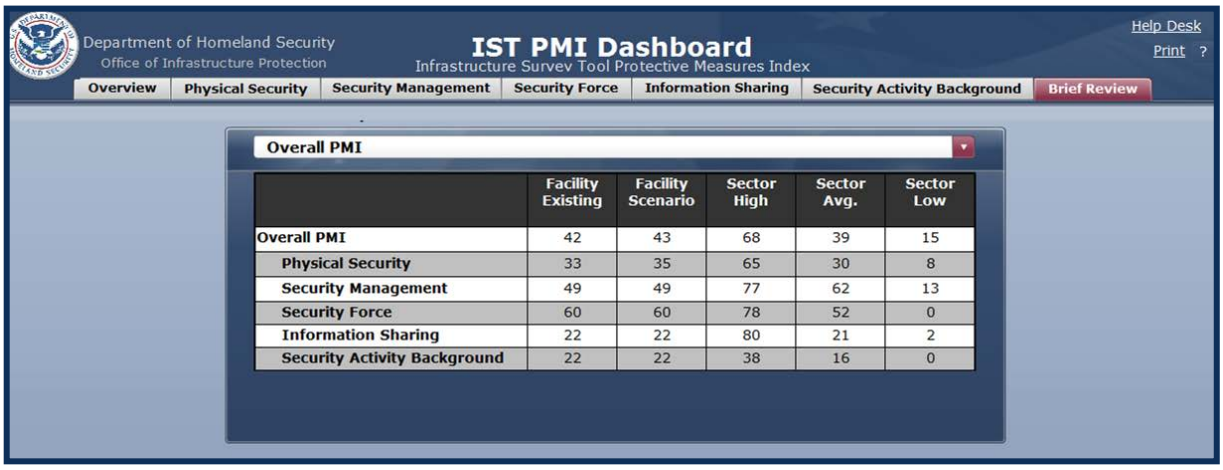


Figure 12: PMI Dashboard Selections: Physical Security/Fences/Fraction Enclosed (Illustrative Asset)

In the bottom-left area of Figure 12, two bars show the existing and the scenario values for the Overall PMI and the Level 1 component selected (i.e., Physical Security). A gauge below the bars shows the value of the Level 2 subcomponent selected (i.e., Fences). In the bottom-right area, a graph displays index values for the existing facility (dark blue), scenario facility (light blue), and sector average (grey) for the Level 3 subcomponents of the Level 2 category. In the middle of the screen, the dashboard displays the information collected characterizing the fraction enclosed. The user may change this information for evaluating a scenario, and then the color of the selection changes from a dark blue to a light blue. In the example presented, the selection (top middle of the screen) indicates that 100 percent of the facility and Significant Assets/Areas (SAAs) are enclosed. The selection is in light blue, which indicates that it is not the current condition at the facility but the user wanted to assess the impact of this measure on the facility's physical security and the overall PMI.

The last type of display available in the PMI Dashboard is the Brief Review, which is illustrated in Figure 13. This display presents different tables combining the values (facility existing, facility scenario, sector high, sector average, and sector low) for the two first levels (i.e., Level 1 and Level 2) that constitute the PMI. A drop-down menu allows the user to select the table to display.



	Facility Existing	Facility Scenario	Sector High	Sector Avg.	Sector Low
Overall PMI	42	43	68	39	15
Physical Security	33	35	65	30	8
Security Management	49	49	77	62	13
Security Force	60	60	78	52	0
Information Sharing	22	22	80	21	2
Security Activity Background	22	22	38	16	0

Figure 13: PMI Dashboard's Brief Review Screen (Illustrative Asset)

The ability to change the parameters, the speed with which users can see the results, and the possibility for assessing different scenarios all serve to make the PMI Dashboard a very powerful tool and particularly relevant for helping to manage protection-related decisions about critical infrastructure facilities.

Facility-specific PMIs demonstrate the potential effectiveness of measures for a particular facility. The list of common options identified through comparison with other like facilities is intended to assist managers in making decisions regarding a site-specific protective measures strategy. No two facilities are alike — each facility's security staff and management team must determine the appropriate combination of measures on the basis of its own assessment of risks, taking into consideration threat, specific assets to be protected, consequences, resilience, facility characteristics, business impacts, return on investment, and overall vulnerability and protection.

The PMI can be used by itself or in combination with other tools or indices for assessing risk at facility or regional levels.

This page intentionally left blank.

4 Use of the Protective Measures Index

The PMI was developed for assessing the capabilities of a facility in terms of protection. This indicator can be used:

- Alone for addressing the protection of a specific facility;
- In combination with other indices (RMI and CMI) to characterize overall risk; and
- For guiding decisions for special events and domestic incidents.

The PMI, used independently of other indices, identifies the elements currently implemented by the facility that contribute to protection (physical security, security management, security force, information sharing, and security activity history/background), compares these elements with what is typically in place for the same type of facility, and assesses different measures for improving the protection level of the facility.

In the broader context of risk assessment, the PMI can be used in combination with other indices developed by Argonne National Laboratory, including the RMI, which addresses elements characterizing preparedness, mitigation measures, response capabilities, and recovery mechanisms, and CMI, which characterizes the maximum consequences.

Figure 14 shows how the PMI and RMI can be combined to support decision-making by critical infrastructure owners and operators. It presents the PMI and RMI values for 12 sites.

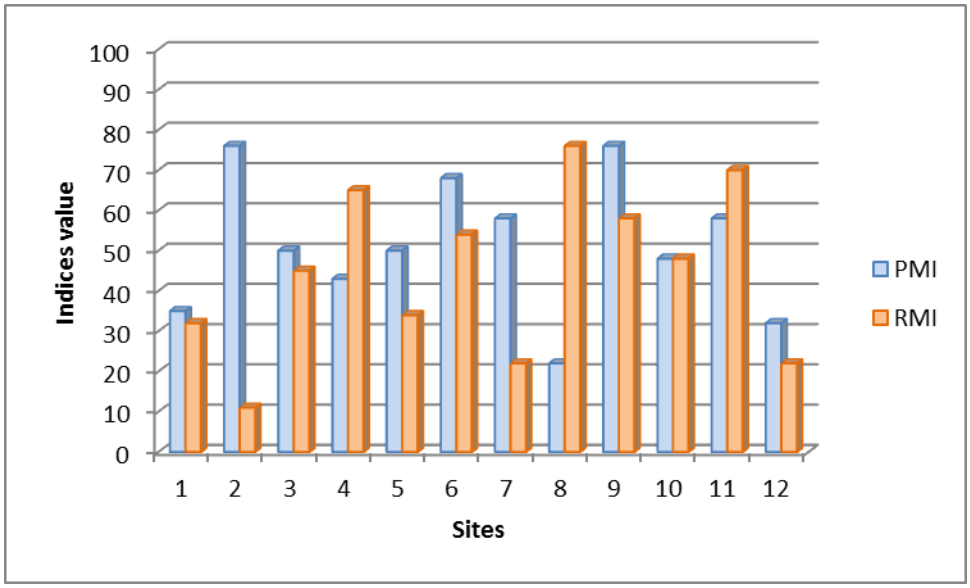


Figure 14: Comparison of Resilience and Protective Measures Indices for 12 facilities (Illustrative)

This type of graph allows users to compare the characteristics of different facilities. Site 8, for example, presents a relatively low PMI and high RMI. This observation may indicate that although the facility has fewer protective measures in place than others, possibly owing to its

location or mission, it has a relatively high level of resilience. This protective stance may be by design, in that the owners realize there may be little they can do to protect the facility or prevent an event, so they have placed more emphasis on being resilient, i.e., responding and recovering as soon as possible. For Site 2, the opposite is true. The relatively high PMI indicates that the facility has emphasized protection and prevention while expending minimal effort on resilience. This score may reflect a deliberate decision because of the type of facility, or the PMI and RMI may identify these qualities to the owner for the first time. Each facility is different and will mitigate vulnerabilities and implement protective and resilience measures on the basis of an individualized assessment of risks, taking into consideration threat, operational needs and other facility characteristics. DHS researchers, analysts, and PSAs recognize that it is not appropriate to implement all mitigation or protective measures at every facility. Therefore, simply raising the index by adding an item does not necessarily correlate directly with achieving a reduction in vulnerability or an increase in resilience for a particular facility unless it is an appropriate measure, properly integrated with the facility's current security and operational posture, and effectively implemented. PMIs or RMIs reflect common protective and resilience measures in place at other similar facilities.

Dashboard comparisons identify facility security and resilience components that are below the subsector average which provides areas for facility management to investigate that may enhance their protection or resilience. There may be very good reasons why a facility will have a component PMI or RMI that is low. For instance, at an urban facility, where parking is allowed on the street and hence the parking standoff distance is small, the facility would simply make note of the vulnerability, which is under the control of the local government, and consider other enhancements to protective measures (e.g., additional closed-circuit television along the facility street-side to identify suspicious vehicles). In terms of resilience, another example might be a facility, such as a hotel, hospital or arena that is not able to maintain an alternative location.

For a given threat type, the risk at a site depends on (1) the threat likelihood, (2) the site's vulnerability (the likelihood that the threat event will be successful), and (3) the magnitude of the consequences of a successful threat event. Increased resilience does factor into this risk determination by lowering the magnitude of consequences. The RMI can therefore be used in conjunction with other indices for risk assessment. The PMI provides a measure of vulnerability, and the CMI provides a measure of the gross (absent any resilience measures) consequences of a successful attack at a site. The RMI can be used to modify the level of consequences to provide a measure of the net consequences at a site due to its resilience measures. Furthermore, for manmade threat events, the threat likelihood should be modified by the consequences at the sites that might be attacked so as to obtain an overall assessment of site risk (see Phillips et al., 2012). Hence, the PMI, together with the other indices, provides a comprehensive representation of infrastructure risk.

Even if the PMI is primarily utilized at facility level, this indicator is also a major component of the Special Event/Domestic Incident Tracker (SEDIT). SEDIT takes a regional approach; it is used not only as a steady-state planning tool but also for impending special events or domestic incidents in which real-time actions must be taken. This tool is used during the advance warning period for a natural hazard, such as a hurricane, or for a special event, such as a major sporting event, and for planning scenarios such as annual flooding. These events can generate increased

risk for critical infrastructure and may require the establishment of new protective or resilience measures for the duration of the events or to increase awareness of infrastructure protection and resilience components when implementing response and recovery activities. SEDIT allows PSAs to take into account real-time threat information and existing facility security and resilience stature, as well as temporary measures as they are put in place, and to analyze their impact on the overall risk of the event.

All of the developed indices provide information that can assist owners and operators in developing a risk-based picture that identifies facility gaps and aids in making informed decisions concerning the protection and resilience of their facility. The PMI is specifically used to assist critical infrastructure owners and operators in (1) analyzing existing protective measures at facilities, and (2) identifying potential ways to increase protection levels of facilities.

This page intentionally left blank.

5 Methodology Advantages and Limitations

The decision analysis methodology used to define the PMI was specifically developed to integrate the major elements necessary to assess the protection of critical infrastructure. The methodology integrates not only physical elements that are traditionally part of protection analysis methodologies but also operational elements, such as security management, security plan, and information-sharing mechanisms. The weighted values of the index are based on a general protective measure framework, which, through consistent application, allows for an index that is suitable for all infrastructure sectors and subsectors.

By organizing the protective measures components into different levels of information and by ranking the relative importance of these components in terms of physical security, security management, security force, information sharing, security activity history/background, and ultimately protective measures, the methodology also ensures the ability to generate reproducible results. Furthermore, by defining a consistent index for protective measures, owners and operators can compare different assets in the same sector, and oversight or coordinating bodies can formulate regional and sector security planning. These comparisons also highlight differences in the way sectors approach protection.

The PMI index allows comparison between critical infrastructure assets but also characterization of the most effective measures for improving protection. The PMI Dashboard lends additional significance to that value and what it means for a facility's overall protective posture. The PMI Dashboard allows owners and operators to take the information that emerges from calculating the indices and utilize it for day-to-day operations, as well as for justification of investment in protection measures and for strategic planning. A sound protective measures assessment methodology is useless if critical infrastructure owners and operators see little or no reason to use it.

Finally, the flexibility of the methodology allows it to be used in different programs developed by DHS to assess the protection and vulnerability of an area or the risk related to a special event. It allows for reproducible results; comparison of critical infrastructure protection derived from consistent methods; and a flexible approach that can be augmented to fit the individual needs of sectors, subsectors, regions, or systems. This methodology also allows DHS to capture a more accurate overall picture of the protection of the Nation's critical infrastructure.

When developing the PMI, comparisons were performed with different standards/approaches to improve the methodology. In 2009, the New York City Police Department prepared a report to support the New York City building community by providing information on how to prevent and mitigate the effects of a terrorist attack on a building (New York Police Department, 2009). Some buildings were designated as "High Tier," based on assessed threat, vulnerability, and impact levels. Recommendations for protective measures for those buildings were included in the report. Most of the recommendations addressed traditional threats from explosive devices, including guidelines on enhancing perimeter security; achieving robust building design; designing effective access control, screening, and monitoring systems; and developing fire-resistance, emergency egress, and communication system solutions. The recommendations also addressed emerging threats from chemical, biological, and radiological weapons, including

guidelines on deploying and using heating, ventilation, and air conditioning systems and associated detection devices.

After reviewing the report, an attempt was made to translate the facts and intent of the document to the calculation of the PMI. For example, the report recommends background checks. Therefore, it was assumed that building owners and operators would adopt the best possible posture for background checks that is specified in the IST (the IST considers several levels of background checks and how often they recur). Similarly, the recommendations indicated that the best possible scores were appropriate for the elements contributing to Information Sharing (e.g., MOU/MOA and exchange of information with local and federal agencies) and Security Activity History/Background (e.g., prior vulnerability assessment and additional protective measures). However, it was necessary to make reasonable assumptions in many cases for the IST/PMI because specific comparable information was not available in the New York City Police Department report.

The results from the report for the general threat showed that Physical Security is the weakest of the five Level 1 components (neglecting dependencies, which were not discussed at all[7]). This result occurred because the New York Police Department has no fences, and discussions of gates, parking, and vehicle access control were minimal; therefore, scores in those areas are low. However, protective measures related to physical security that owners and operators could reasonably be expected to implement resulted in very high PMI scores for access control and lighting.

The primary use of the results of this exercise was to provide perspective and a level of comparison for buildings being surveyed by DHS PSAs using the IST during the early days of the DHS surveys. It was generally assumed that implementation of protective measures recommended by the New York City Police Department for high-risk buildings should be a relatively desirable level of achievement for most buildings. For example, for these high-risk buildings, the Security Management PMI was 83, and the Security Force PMI was 94. However, as noted above, some protective measures included in the IST are not practical for buildings, and therefore, perfect or near-perfect scores should not be expected for all subcomponents of the PMI. These results for high-risk New York City buildings were helpful to owners and operators as they reviewed PMI results for their own buildings.

Although the PMI has many advantages, it also presents some limitations. These limitations are not directly related to the process of calculation or to the PMI organizational structure. The notions of physical security, security management, security force, information sharing, and security activity are self-explanatory and are well understood in the field of security and risk management. Furthermore, MAUT and decision analysis concepts have become standard in the domain of risk assessment and management; see, for example, the Decision Analysis and Risk Specialty Group of the Society for Risk Analysis (SRA, 2013). The main limitations of this tool

[7] Previous versions of the PMI combined six Level 1 components: Physical Security, Security Management, Protective Measures Background, Security Force, Information Sharing, and Dependencies. These Level 1 components have been redefined in the current version of the PMI, which combines five Level 1 components: Physical Security, Security Management, Security Force, Information Sharing, and Security Activity History/Background. Information collected for dependencies is now used exclusively for the RMI calculation.

relate to the way the results may be misinterpreted or used for unintended purposes. For the interpretation of the value defined with the PMI, it is important to remember that the PMI is a relative indicator of critical infrastructure protection based on information collected over the course of 4 to 8 hours. In addition, because the PMI must be applicable across all infrastructure sectors, the individual assessor's knowledge of a specific facility's technical and operational functions is also a factor. However, the reproducibility of the process is ensured via the training of assessors and by the QA process. The PMI characterizes protection at a specific facility. PMI values defined for different facilities cannot be used directly for defining the overall protection of a specific region or a given sector. Although the PMI of different assets in a region may provide an indication of the level of security in a region, other elements characterizing the region (e.g., population, economy, environment, institutional services) also affect regional protection and vulnerability.

The PMI should be used as part of an overall risk management program. It provides important information about the protective measures implemented at a given facility and how that facility compares to another similar facility. Other factors such as location, specific vulnerabilities, and a cost-benefit analysis should also be utilized to help ensure that a complete picture of a facility's protection level or posture is realized.

This page intentionally left blank.

6 Conclusion

In 2011, Presidential Policy Directive 8 (DHS, 2011) underscored national preparedness for strengthening the security and resilience of the Nation. It promoted an all-hazards approach based on a definition of the core capabilities facilities needed to possess to be better prepared. It also reaffirmed the shared responsibility of all levels of government, the private sector, and individual citizens in the Nation to enhance preparedness. Critical infrastructure is directly mentioned in the document for two specific types of capabilities: protection, which refers to the "necessity to secure the homeland against acts of terrorism and manmade or natural disasters," and mitigation, which is the "necessity to reduce loss of life and property by lessening the impact of disasters." In 2013, Presidential Policy Directive 21 (White House, 2013) reinforced the need to address the security and resilience of critical infrastructure in an integrated, holistic manner to reflect interconnectedness and interdependency. This directive states that critical infrastructure must be secure and able to withstand and rapidly recover from all hazards. It particularly stresses physical and cyber threats and required efforts to reduce vulnerabilities, minimize consequences, identify and disrupt threats, and hasten response and recovery efforts.

The enhancement of the PMI is directly aligned with this need to address the capabilities of critical infrastructure in terms of security and protection. The PMI is intended to assist DHS in analyzing the protection of the Nation's critical infrastructure and identifying ways to improve it. Its associated index — the VI — provides an indication of the vulnerability of critical infrastructure. The PMI and VI provide valuable information to critical infrastructure facility owners and operators about their standing relative to similar sector assets and about various ways to enhance the protection and security of their facilities. Applications and uses of the PMI for DHS programs continue to evolve, and concept improvements and additional enhancements and approaches are expected. Combining the PMI with other indices (RMI and CMI) provides additional benefits, including allowing for an overall view of risk. The objective is to develop better decision-making tools that facilitate comparison of critical infrastructure assets and promote a proactive approach to improving preparedness, protection, mitigation, response, and recovery capabilities.

This page intentionally left blank.

7 References

ASIS (ASIS International), 2012, *Protection of Assets*, ASIS International, Alexandria, Virginia, available at https://poa.asisonline.org/Purchase-Protection-of-Assets/Pages/Print-Bundle.aspx, accessed July 18, 2013.

DHS (U.S. Department of Homeland Security), 2009, *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency*, Washington, D.C., available at http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf, accessed July 18, 2013.

DHS, 2010, *DHS Risk Lexicon – 2010 edition*, Washington, D.C., available at http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf, accessed July 18, 2013.

DHS, 2011, *Presidential Policy Directive/PPD-8: National Preparedness*, Washington, D.C., available at http://www.dhs.gov/presidential-policy-directive-8-national-preparedness, accessed July 18, 2013.

DHS, 2013a, *Protected Critical Infrastructure Information (PCII) Program*, Washington, D.C., available at http://www.dhs.gov/protected-critical-infrastructure-information-pcii-program, accessed July 18, 2013.

DHS, 2013b, *Site Assistance Visits*, Washington, D.C., available at http://www.dhs.gov/site-assistance-visits, accessed July 18, 2013.

Ezell, B.C., 2007, *Infrastructure Vulnerability Assessment Model (I-VAM)*, Risk Analysis, Vol. 27, No. 3, pp.571–583.

FEMA (Federal Emergency Management Agency), 2003, *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings –Providing Protection To People and Buildings*, Risk Management Series, FEMA 426, Dec., Washington, D.C.

FEMA, 2005, *Risk Assessment – A How-To Guide to Mitigate Potential Terrorist Attacks Against Buildings – Providing Protection To People and Buildings*, Risk Management Series, FEMA 452, Jan., Washington, D.C.

Fisher, R.E., W.A. Buehring, R.G. Whitfield, G.W. Bassett, D.C. Dickinson, R.A. Haffenden, M.S. Klett, and M.A. Lawlor, 2009, *Constructing Vulnerability and Protective Measures Indices for the Enhanced Critical Infrastructure Protection Program*, Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-09-4, Argonne, Ill, USA.

Fisher, R.E., G.W. Bassett, W.A. Buehring, M.J. Collins, D.C. Dickinson, L.K. Eaton, R.A. Haffenden, N.E. Hussar, M.S. Klett, M.A. Lawlor, D.J. Miller, F.D. Petit, S.M. Peyton, K.E. Wallace, R.G. Whitfield, and J.P. Peerenboom, 2010, *Constructing a Resilience Index for the Enhanced Critical Infrastructure Protection Program*, Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-10-9, Argonne, Ill, USA.

GAO (U.S. Government Accountability Office), 2007, *Homeland Security: Applying Risk Management Principles to Guide Federal Investments*, Testimony before the Subcommittee on Homeland Security, Committee on Appropriations, House of Representatives.

GAO, 2008a, *Risk Management: Strengthening the Use of Risk Management Principles in Homeland Security*, Testimony before the Subcommittee on Transportation Security and Infrastructure Protection, Homeland Security Committee, House of Representatives.

GAO, 2008b, *Homeland Security: DHS Risk-Based Grant Methodology is Reasonable but Current Version's Measure of Vulnerability is Limited*, Report to Congressional Committees.

Interagency Security Committee, 2010, Physical Security Criteria for Federal Facilities: An Interagency Security Committee Standard (FOUO), Washington, D.C.

Keeney, R.L., 1992, *Value-Focused Thinking: A Path to Creative Decisionmaking*, Harvard University Press, Cambridge, Mass.

Keeney, R.L., and H. Raiffa, 1976, *Decisions with Multiple Objectives: Preferences and Value Tradeoffs*, John Wiley and Sons, New York, New York.

New York Police Department, 2009, *Engineering Security – Protective Design for High-Risk Buildings*, The City of New York, New York City Police Department, New York City, NY, 130 p., available at http://www.veilig-ontwerp-beheer.nl/publicaties/engineering-security-protective-design-for-high-risk-buildings/view, accessed July 18, 2013.

Petit, F.D, G.W. Bassett, R. Black, W.A. Buehring, M.J Collins, D.C. Dickinson, R.E. Fisher, R.A. Haffenden, A.A. Huttenga, M.S. Klett, J.A. Phillips, M. Thomas, S.N. Veselka, K.E. Wallace, R.G. Whitfield, and J.P. Peerenboom, 2013, *Resilience Measurement Index: An Indicator of Critical Infrastructure Resilience*, Argonne National Laboratory, Decision and Information Sciences Division, ANL/DIS-13-01, 70 p.

Petit, F., L. Eaton, R. Fisher, S. McAraw, and M. Collins, 2012, "Developing an Index to Assess the Resilience of Critical Infrastructure," *International Journal of Risk Assessment and Management* (IJRAM), Inderscience Publishers, Geneva, Switzerland, Vol. 16, Nos. 1/2/3, pp. 28–47.

Petit, F., R. Fisher, W. Buehring, R. Whitfield, and M. Collins, 2011, "Protective Measures and Vulnerability Indices for the Enhanced Critical Infrastructure Protection Program," *International Journal of Critical Infrastructures* (IJCIS), Inderscience Publishers, Geneva, Switzerland, Vol. 7, No. 3, pp. 200–219.

Phillips, J.A., G.W. Bassett, W.A. Buehring, J.L. Carlson, R.G. Whitfield, and J.P. Peerenboom, 2012, "A Framework for Assessing Infrastructure Risk," M4-I Resilience Evaluation Approaches for the Analysis of Complex Systems, Risk Analysis: Advancing Analysis, Society for Risk Analysis, 2012 Annual Meeting, Dec. 9–12, San Francisco, Calif.

Snyder, J.L., 2009, *The Mumbai Attacks: A Wake-up Call for America*, *testimony of James L. Snyder*, Deputy Assistant Secretary for Infrastructure Protection, National Protection and Programs Directorate, before the House Committee on Homeland Security Subcommittee on Transportation Security and Infrastructure Protection, March 11, available at http://www.dhs.gov/ynews/testimony/testimony_1237299957226.shtm, accessed July 18, 2013.

SRA (Society for Risk Analysis), 2013, *Decision Analysis and Risk Specialty Group*, available at http://www.sra.org/darsg, accessed July 18, 2013.

White House, 2013, *Presidential Policy Directive — Critical Infrastructure Security and Resilience*, Presidential Policy Directive/PPD-21, Washington. D.C., available at http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil, accessed July 18, 2013.

This page intentionally left blank.

Appendix A: Protective Measures Index Structure

The schematic in Figure A1 shows the relevant Level 1 components, Level 2 subcomponents, and number of Level 3 subcomponents of the Protective Measures Index (PMI).

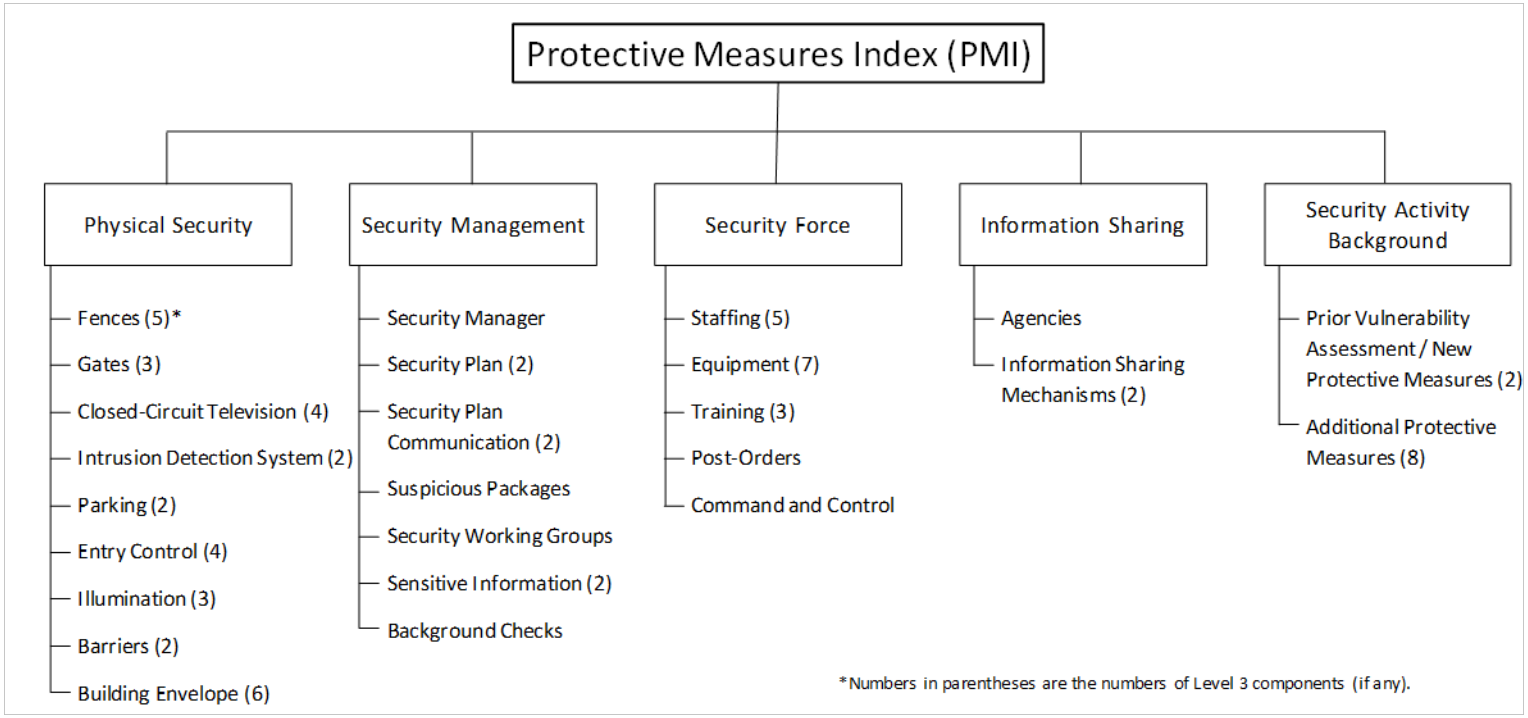


Figure A1: Structure of the PMI Level 1 Components and Level 2 and 3 Subcomponents

This page intentionally left blank.

Appendix B: Illustration of Weight Determination[8]

The Protective Measures Index (PMI) is defined by the aggregation of four levels of information. Each type of data collected and each element comprising Levels 4 through 1 have been weighted by subject matter experts (SMEs) to represent the relative importance of components and subcomponents compared with other data in the same groupings by considering their contribution to the overall protective posture of critical infrastructure. The weights for a set of subcomponents depend on the ranges (worst to best) of each subcomponent compared with others in the same set. The weights characterize a general sector (or subsector) and a general threat.[9] For example, seven elements are considered for defining the type of exercises that can be used for the security plan:

- Tabletop with external responders;
- Tabletop without external responders;
- Functional with external responders;
- Functional without external responders;
- Full-scale with external responders;
- Full-scale without external responders; and
- Post-exercise/event analysis.

Table B1 presents the ranks and relative importance defined by three teams of SMEs for these seven elements during the elicitation process.

[8] This appendix demonstrates the arithmetic of the calculation. Values are shown to several decimal places to allow readers to follow the calculation. Use of one or more significant figures does not imply accuracy at the same level.

[9] Specific Level 1 and Level 2 weights have also been defined for specific sectors and threats — see Appendix C.

Table B1: Ranks and Relative Importance Defined by SMEs for the Security Plan Exercises Subcomponents

Type of Exercise	Team 1		Team 2		Team 3	
	Rank	Relative Importance	Rank	Relative Importance	Rank	Relative Importance
Tabletop (practical or simulated exercise)—does not include external responders.	7	20	7	40	6	60
Tabletop—includes external responders.	6	30	5	50	5	65
Functional (walk-through or specialized exercise)—does not include external responders.	5	50	5	50	4	75
Functional—includes external responders.	4	60	4	60	2	95
Full-scale (simulated or actual event)—does not include external responders.	2	80	2	80	3	90
Full-scale—includes external responders.	1	100	1	100	1	100
Exercise or actual event results are documented; corrective actions are identified and reported to executive management.	2	80	2	80	7	30

All teams agree that the most important element in terms of protection is the realization of full-scale exercises in partnership with external responders. Full-scale exercise without external responders is ranked second by two of the teams and third by team 3, which prefers functional exercises with external responders. The main difference among the three teams is the relative importance of the post-exercise/event analysis, which is ranked second by teams 1 and 2 and seventh by team 3. Values vary from 20 to 100 for team 1, 40 to 100 for team 2, and 30 to 100 for team 3. Team 3 assigns relatively close values except for the one defined for post-exercise/event analysis, which is lower, with a relative importance of 30.

Once the SME teams have defined the ranks and relative values for a given set of information, a period of discussion allows them to exchange and explain the elements that guided their thinking. On the basis of this discussion, the SMEs can review the ranks and relative values defined. On the basis of the values and ranks, a global relative value is defined for each subcomponent. In our illustrative example, Table B2 presents the overall relative importance defined for the seven elements characterizing the security plan exercises.

Table B2: Notional Relative Importance Obtained for Subcomponents of the Security Plan Exercises

Type of Exercise	Rank	Relative Importance
Tabletop (practical or simulated exercise)—does not include external responders.	7	38.3
Tabletop—includes external responders.	6	46.9
Functional (walk-through or specialized exercise)—does not include external responders.	5	57.2
Functional—includes external responders.	4	70.1
Full-scale (simulated or actual event)—does not include external responders.	2	82.9
Full-scale—includes external responders.	1	100
Exercise or actual event results are documented; corrective actions are identified and reported to executive management.	3	74.3

In terms of final ranking and relative importance values, a full-scale exercise with first responders is still the most important subcomponent of this grouping, with a rank of one and a value of 100. The least important element, in comparison with others in the grouping, is the tabletop exercise without external responders, with a value of 38.3. The global relative importance values are not a direct average of the values defined by the SMEs; rather, the values integrate the ranking and then the relative importance of each element. For example, the relative importance for the post-exercise/event analysis is not 63.33, which corresponds to the average of the values defined by the SMEs, but 74.3, which incorporates the fact that two teams of SMEs ranked this element second.

When the relative importance of each element in a set is defined, the weights can be calculated by using a cross multiplication. The weights vary between 0 and 1, and must add up to 1 in a given set. Table B3 presents the overall weights for the seven elements characterizing the security plan exercises.

Some options in the type of exercises are mutually exclusive. For example, a tabletop exercise cannot be conducted both with and without external responders. Therefore, exercises without external responders, which have lower relative importance than exercises with external responders, are not considered for defining the sum of the relative importance. Thus, the relative importance of exercises with external responders and post-exercise/event analysis are added to define the overall sum that is used for calculating the weights. Indeed, the weights of these elements add to one.

Table B3: Notional Weights Obtained for Subcomponents of the Security Plan Exercises

Level 4 Subcomponent	Rank	Relative Importance	Weight[a]
Tabletop (practical or simulated exercise)—does not include external responders.	7	38.3	*0.131*
Functional (walk-through or specialized exercise)—does not include external responders.	5	57.2	*0.196*
Full-scale (simulated or actual event)—does not include external responders.	2	82.9	*0.285*
Tabletop—includes external responders.	6	**46.9**	**0.161**
Functional—includes external responders.	4	**70.1**	**0.241**
Full-scale—includes external responders.	1	**100**	**0.343**
Exercise or actual event results are documented; corrective actions are identified and reported to executive management.	3	**74.3**	**0.255**
Sum:		**291.3**	**1**

[a] In discussions of the PMI, several decimal places are shown to allow the audience to follow the arithmetic, if desired, and clarify the methodology. These are not meant to imply a high degree of precision or confidence in the value judgments elicited from SMEs or related protection estimates.

The same exercise is repeated for each subcomponent of the PMI. Table B4 presents the overall weights obtained for the Level 1 components of the PMI.

Table B4: Notional Weights Obtained for the PMI Level 1 Components

Level 1 Component	Rank	Relative Importance	Weight
Physical Security	2	88.85	0.271
Security Management	1	100	0.305
Security Force	3	80	0.244
Information Sharing	4	33.11	0.101
Security Activity History/Background	5	25.90	0.079
Sum:		327.86	1

The most important contributor to the overall PMI is Security Management, with a relative importance of 100, followed by Physical Security (88.85), Security Force (80), Information Sharing (33.11), and Security Activity History/Background (25.90).

This page intentionally left blank.

Appendix C: Sector and Threat Dependencies of the Weights

Weights for Level 1 components and Level 2 subcomponents depend on sector, or subsector, and threat. The weights obtained to date from the sectors and the protective security advisors (PSAs) have verified this fact. Table C1 shows the physical security subcomponents weights (Level 2 weights) obtained from the PSA group for general, improvised explosive device (IED), and vehicle-borne improvised explosive device (VBIED) threats.

Table C1: PSA Physical Security Subcomponent Weights as a Function of Threat

	Level 2 Subcomponents Weights		
Physical Security Subcomponents	General Threat	IED	VBIED
Fences	0.116	0.135	0.123
Gates	0.134	0.135	0.133
Closed-Circuit Television	0.082	0.076	0.082
Intrusion Detection System	0.100	0.111	0.073
Parking	0.082	0.078	0.130
Entry Control	**0.148**	**0.148**	0.116
Illumination	0.110	0.101	0.101
Barriers	0.128	0.115	**0.144**
Building Envelope	0.100	0.101	0.098

While entry control is the most important subcomponent for general and IED threats, barriers are the most important for a VBIED threat. Also notable is that the intrusion detection system subcomponent is more important for general and IED threats than for a VBIED threat, and that parking is more important for a VBIED threat than for general and IED threats.

Weights can also vary by sector. Table C2 presents the physical security subcomponent weights as a function of sector considering a VBIED threat.

Table C2: PSA Physical Security Subcomponent Weights as a Function of Sector

	Level 2 Subcomponents Weights		
Physical Security Subcomponents	VBIED – General Sector	VBIED – Commercial Facilities Sector	VBIED – Chemical and Hazardous Materials Industry Sector
Fences	0.123	0.044	0.116
Gates	0.133	0.054	0.133
Closed-Circuit Television	0.082	0.141	0.066
Intrusion Detection System	0.073	0.091	0.084
Parking	0.130	**0.163**	0.132
Entry Control	0.116	0.127	0.124
Illumination	0.101	0.114	0.108
Barriers	**0.144**	0.155	**0.141**
Building Envelope	0.098	0.111	0.096
Sum:	1	1	1

Barriers remain an important subcomponent for the General, Commercial Facilities, and Chemical and Hazardous Materials Industry Sectors but are less important than parking for the Commercial Facilities Sector. Fences and gates are significantly more important for the Chemical and Hazardous Materials Industry Sector than for the Commercial Facilities Sector. On the other hand, closed-circuit television is much more important for the Commercial Facilities Sector than for the Chemical and Hazardous Materials Industry Sector. These results for the PSA group demonstrate that physical security Level 2 weights depend on sector and threat, as expected.

To date, Level 1 weights in general have not shown a strong dependency on sector and threat. For the PSA group, the Level 1 weights did not vary for IED and VBIED threats for the Commercial Facilities and Chemical and Hazardous Materials Industry Sectors. However, for the Healthcare and Public Health Sector, six subsectors were defined, and Level 1 weights did vary somewhat over the threat categories examined.

In a few instances for the Healthcare and Public Health Sector, a strong dependency of Level 1 weights on threat was observed. For example, security force was among the most important of the Level 1 weights for five of the six Healthcare and Public Health subsectors; however, for the Fatality/Mortuary Facility subsector, security force had the lowest weight of the five Level 1 components (Table C3).

Table C3: PSA PMI Component Weights as a Function of Subsector – Healthcare and Public Health Sector

	Level 1 Components Weights						
Level 1 Components	VBIED – Healthcare and Public health Sector	VBIED – Direct Patient Healthcare	VBIED – Regulatory, oversight, or Industry Organization	VBIED – Medical Supplies, Devices, or Equipment	VBIED – Fatality/Mortuary Facility	VBIED – Medical and Diagnostic Laboratory	VBIED – Public Health Agency
Physical Security	0.213	0.182	0.182	0.253	0.227	0.253	0.182
Security Management	0.276	0.259	0.259	0.253	0.377	0.253	0.259
Security Force	0.201	0.221	0.221	0.228	0.075	0.228	0.221
Information Sharing	0.221	0.234	0.234	0.203	0.227	0.203	0.234
Security Activity History/Background	0.089	0.104	0.104	0.063	0.094	0.063	0.104
Sum:	1	1	1	1	1	1	1

This page intentionally left blank.

Appendix D: Example of Calculation Rollup[10]

The PMI is an aggregation of information from questions answered during a facility visit to an overall index. The information is collected using yes/no questions, that is, either the element is present or not. For the calculation of whether a specific element is present or if the answer to a question is "Yes," this element is given a value of 100. If the element is not present or if the answer to a question is "No," this element is given a value of 0. Table D1 presents an example of this information for Fences Type.

Table D1: Fences Type Index (Illustrative Asset)

Fences Type Subcomponents – Level 4	Answer	Value	Level 4 Weights	Weighted Index
Aluminum or Steel Chain Link	Yes[a]	100	0.5	50
Anti-Climb Aluminum or Steel Chain Link	No[b]	0	0.8	0
Steel – Not Chain Link	No	0	0.75	0
Wood	No	0	0.25	0
Concrete	No	0	1	0
Wrought Iron	No	0	0.4	0
Brick and Mortar	No	0	1	0
Plastic	No	0	0.1	0
Level 3 Fences Type Index (FTI)			**Value:**	**50**

[a] "Yes" means that the element is implemented, and it is given a numerical value of 100.
[b] "No" means that the element is not implemented, and it is given a numerical value of 0.

The types of material used for the fences are mutually exclusive. In consequence, it is not necessary to have fences with all types of material to get the best Fences Type Index (FTI). The best option in terms of protection is to have fences constructed of concrete or brick and mortar (weight of 1). The worst option is to have a fence constructed of plastic (weight of 0.1). If the fence is made of another material, the user must select the type of material in the list that is closest to the one used.

Collected data are aggregated to define an FTI, a Level 3 component of the PMI, by using Equation 1.

$$FTI = \sum_{i=1}^{8} a_i \times Z_i \qquad (1)$$

where:

FTI = fences type index, Level 3 (ranging from 0 to 100);

[10] This appendix demonstrates the arithmetic of the calculation. Values are shown to several decimal places to allow the reader to follow the calculation. Use of one or more significant figures does not imply accuracy at the same level.

a_i = scaling constant (weight) indicating the relative importance of possibility i (i = 1,2,3,4, 5, 6, 7, 8) for fences type; and
Z_i = value of component i of fences type (0, if not present, or 100, if present).

In the example, the facility's weakest fence is made of aluminum chain link, which gives, by using equation 1, an overall FTI of 50 (Table D1).

Level 3 subcomponents are aggregated into Level 2 subcomponents, which represent the main characteristics of the facility studied, such as its access control, staffing, and security plan. For example, the fences type component, Level 3, is one subcomponent of the Level 2 fences subcomponent (Table D2).

Table D2: Fences Index (Illustrative Asset)

Fences Subcomponents – Level 3	Level 3 Index	Level 3 Weights	Weighted Index
Fences Type	**50**	0.313	15.65
Fences Height	10	0.280	2.80
Base of Fence	100	0.188	18.8
Other Characteristics	46.48	0.219	10.18
Level 2 Fences Index (FI)		**Value:**	**47.43**

On the basis of the Level 3 weights, the fences type is the most important elements with a weight of 0.313. The less important is the base of the fence with a weight of 0.188. The facility in the example is fully enclosed by a 5-foot fence with an anchored base; however, there are no outriggers (barbed wire or razor wire) or any specific enhancement (e.g., spikes, electric, or second fence). The fence is surrounded by a clear zone free of objects, and warning signs are placed on the perimeter.

Level 3 subcomponents are combined to create a Level 2 index. The fences index (FI) (Level 2) is obtained by using Equation 2.[11]

$$FI = \sum_{i=1}^{4} b_i \times Y_i \qquad (2)$$

where:
FI = fences index, Level 2 (ranging from 0 to 100);
b_i = scaling constant (weight) indicating the relative importance of possibility i (i = 1, 2, 3, 4) for fences; and
Y_i = value of component i of fences

[11] The subcomponent "Fraction Enclosed" acts as a multiplier. If the facility and the SAAs are fully enclosed, the value of FI is the result of the weighted sum (Equation 2). If the facility and the SAAs are both not fully enclosed, the FI is attributed a value of 0. If only one of the elements (the facility or SAAs) is fully enclosed, the value of FI is defined by a fraction of the value obtained with Equation 2.

The relative importance (weight) of Fences Type is 0.313. By multiplying the value of the FTI (50) by its weight, a weighted FTI value of 15.65 is obtained. This value is added to the other weighted index that constitutes the Fences subcomponent (Level 2) to obtain an overall FI of 47.43 (Table D2).

Level 2 components are aggregated to define Level 1 components, which represent the five main concepts of protective measures (Appendix A):

Physical Security. This Level 1 component groups Level 2 subcomponents that characterize fences, gates, closed-circuit television, intrusion detection system, parking, entry control, illumination, barriers, and building envelope.

Security Management. This Level 1 component groups Level 2 subcomponents that characterize security plan and planning for suspicious packages, security working groups, sensitive information, and background checks.

Security Force. This Level 1 component groups Level 2 subcomponents that characterize staffing, equipment, training, post orders, and command and control.

Information Sharing. This Level 1 component groups Level 2 subcomponents that characterize information-sharing mechanisms, memoranda of understanding (MOUs), and memoranda of agreement (MOAs).

Security Activity History/Background. This Level 1 component groups Level 2 subcomponents that characterize prior vulnerability assessments and additional protective measures during elevated threat situations.

For the PMI, entry control is the most important subcomponent of physical security, with a weight of 0.148. The least important components of physical security are closed-circuit television and parking, each with a weight of 0.082 (Table D3).

Table D3: Physical Security Index (Illustrative Asset)

Physical Security Subcomponents – Level 2	Level 2 Index	Level 2 Weights	Weighted Index
Fences	**47.43**	0.116	5.50
Gates	29.55	0.134	3.96
Closed-circuit television	28.63	0.082	2.35
Intrusion detection system	22.94	0.100	2.29
Parking	44.51	0.082	3.65
Entry control	65.79	0.148	9.74
Illumination	92.41	0.110	10.16
Barriers	47.43	0.128	6.07
Building Envelope	53.33	0.100	5.33
Level 1 Physical Security Index (PSI)		**Value:**	**49.05**

The facility analyzed in our example has an index of 29.55 for gates, which characterizes standard aluminum swing gates without specific enhancements (e.g., barbed wire, spikes). The index for closed-circuit television is 28.63, which corresponds to a digital and color system that can monitor all critical areas with a good program of maintenance, update, and testing. However, there is no real monitoring or review policy of the information collected. The index for intrusion detection system is 22.94. The facility does not have an exterior intrusion detection system. There is an interior system that allows for detection of glass breakage for doors and windows. This system is continuously monitored both onsite and offsite. The index for parking is 44.51, which corresponds to the presence of uncontrolled parking adjacent and on the street without any specific monitoring. However, there is a specific procedure to identify and act on unauthorized extended-stay vehicles. The index for entry control is 65.79. The facility, in the example, does not allow entry to the public. Access control for personnel, visitors, and contractors is provided by an unarmed guard with credential checks (e.g., government-issued identification [ID] and facility-issued ID) and a sign in/out process. The index for illumination is 92.41, which corresponds to uniform and constant illumination with overlapping light pattern coverage and backup to cover critical locations. However, the facility does not have portable lighting onsite for emergencies or heightened threat levels. The index for barriers is 47.43, which corresponds to the use of jersey barriers (but that are not K-rated) for mitigating a high-speed avenue of approach and enforcing standoff from the facility. Finally, the building envelope index is 53.33, which corresponds to the presence of ground floor windows and the use of metal-framed glass doors without any specific reinforcement or protective measures.

The physical security index (PSI) is calculated as the weighted sum of its nine subcomponents using Equation 3.

$$PSI = \sum_{i=1}^{9} c_i \times X_i \tag{3}$$

where:

PSI = physical security index, Level 1 (ranging from 0 to 100);
c_i = scaling constant (weight) indicating the relative importance of component i (i = 1, 2, 3, 4, 5, 6, 7, 8, 9) of physical security; and
W_i = index value of component i of physical security.

The relative importance (weight) of fences for physical security is 0.116. By multiplying the value of the FI (47.43) by its weight, a weighted FI of 5.50 is obtained. This value is added to the weighted index of the other subcomponent of physical security (Level 1) to obtain a PSI of 49.05 (Table D3).

Finally, the five Level 1 components are aggregated to define an overall PMI (Table D4).

Table D4: Protective Measures Index (Illustrative Asset)

PMI Components – Level 1	Level 1 Index	Level 1 Weights	Weighted Index
Physical Security	**49.05**	0.271	13.29
Security Management	67.70	0.305	20.65
Security Force	66.66	0.244	16.26
Information Sharing	6.04	0.101	0.61
Security Activity History/Background	0	0.079	0
Protective Measures Index (PMI)		**Value:**	**50.81**

According to the overall weights, security management is the most important component of facility protection with a weight of 0.305, while security activity history/background is the least important with a weight of 0.079. Physical security, security force, and information sharing have intermediate importance with respective weights of 0.271, 0.244, and 0.101.

The facility analyzed in the example has an index of 67.70 for security management, which corresponds to the presence of a security manager and a security plan developed at the facility level and approved by senior management. This plan has specific procedures for physical security and security force. Key personnel are trained at initial employment, and tabletop exercises are conducted every year with a report provided to executive management. However, training and exercises do not include law enforcement. The facility has specific procedures for conducting background checks and handling suspicious packages. However, it lacks processes for sensitive information, and the facility does not participate in any security working group.

The facility in the example has a security force index of 66.66, which corresponds to an unarmed security force without arrest or detained authority. The security force is trained semiannually for break-ins, fire, CPR/first aid, and screening and access procedures. Fully 100% of its critical areas are covered by predetermined sequence roving patrols but only 25% of static posts are covered by security force personnel.

The facility in the example has an information-sharing index of 6.04, which corresponds to a facility without MOUs or MOAs with entities other than emergency responders (e.g., neighboring facilities, contract response companies) and that exchanges information procedures with the U.S. Department of Homeland Security (DHS) and local law enforcement only.

The facility in the example has not conducted any vulnerability assessments in the past, and there is no specific procedure for implementing additional protective measures during elevated threat situations. Thus, the security activity history/background for this facility is 0.

The overall PMI consists of a weighted sum of its five Level 1 components (physical security, security management, security force, information sharing, and security activity history/background), as shown in Equation 4.

$$PMI = \sum_{i=1}^{5} d_i \times W_i \quad (4)$$

where:

PMI = relative protective measures index (ranging from 0 to 100);
d_i = scaling constant (weight; a number between 0 and 1) indicating the relative importance of component i (i = 1, 2, 3, 4, 5) of protective measures; and
W_i = index value of component i of protective measures (i.e., physical security, security management, security force, information sharing, and security activity history/background).

The relative importance (weight) of the PSI is 0.271. By multiplying the value of the PSI (49.05) by its weight, a weighted PSI of 13.29 is obtained. This value is added to the other weighted index values of components of protection to obtain an overall PMI of 50.81 (Table D4).

The calculation process results in an overall PMI that ranges from 0 (low protection) to 100 (high protection) for the critical infrastructure analyzed, as well as an index value for each Level 1 through Level 3 components. This method of characterizing the protection level of a critical infrastructure asset allows DHS to not only consider the specificity of all subsectors but also to compare the efficiency of different measures to increase protection in the studied system.

When the PMI is calculated, the Vulnerability Index (VI) can be calculated by using Equation 5:

$$VI = 100 - PMI \quad (5)$$

where:

VI = Vulnerability Index (ranging from 0 to 100);
PMI = Protective Measures Index (ranging from 0 to 100).

When the VI is low, the PMI is high, and vice versa. When an action is taken to increase protection (i.e., moving to the right along the horizontal axis in Figure D1), the PMI rises and the VI decreases. Figure D1 shows that the overall facility PMI in our example is 50.81, which corresponds to a VI of 49.19.

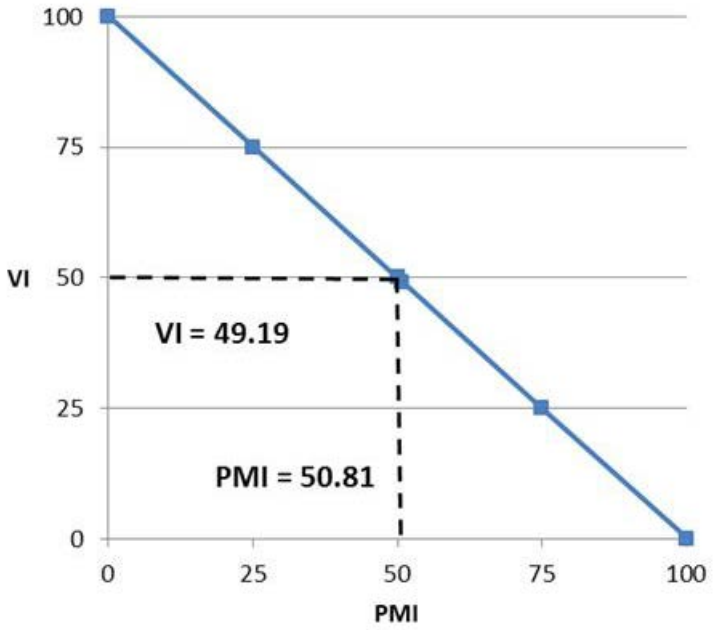


Figure D1: Relationship of Protective Measures Index to Vulnerability Index

It is important to note that a VI equal to 0 does not mean the asset is not vulnerable. Rather, the VI represents the combination of all protective measures, procedures, and policies identified within the Enhanced Critical Infrastructure Protection survey that results in the lowest vulnerability. Thus, the VI is related to, but does not correspond precisely with, the probability of success of an attack, which is sometimes thought of as vulnerability.

This page intentionally left blank.

Appendix E: List of Abbreviations

CMI	consequences measurement index
DHS	U.S. Department of Homeland Security
ECIP	Enhanced Critical Infrastructure Protection (program)
FEMA	Federal Emergency Management Agency
HITRAC	Homeland Infrastructure Threat and Risk Analysis Center
ID	identification
IED	improvised Explosive Device
IST	Infrastructure Survey Tool
MAUT	Multi-attribute utility theory
MOA	memoranda of agreements
MOU	memoranda of understanding
NG	National Guard
PMI	protective measures index
PSA	protective security advisor
PSI	physical security index
QA	quality assurance
RI	resilience index
RMI	resilience measurement index
SAA	Significant Assets/Areas
SAV	site assistance visit
SME	subject matter expert
SEDIT	special event and domestic incident tracker
VBIED	vehicle borne improvised explosive device
VI	Vulnerability Index

This page intentionally left blank.

Decision and Information Sciences Division
Argonne National Laboratory
9700 South Cass Avenue, Bldg. 221
Argonne, IL 60439-4844

www.anl.gov