ANL/DIS-09-4

Constructing Vulnerability and Protective Measures Indices for the Enhanced Critical Infrastructure Protection Program

Decision and Information Sciences Division

ANL/DIS-09-4

Constructing Vulnerability and Protective Measures Indices for the Enhanced Critical Infrastructure Protection Program

by
R.E. Fisher, W.A. Buehring, R.G. Whitfield, G.W. Bassett, D.C. Dickinson,
R.A. Haffenden, M.S. Klett, and M.A. Lawlor
Decision and Information Sciences Division, Argonne National Laboratory, Argonne, Illinois

October 1, 2009

This page intentionally blank

Contents

Figures

Tables

Contents (Cont.)

Acknowledgments

The authors gratefully acknowledge the contributions of many people who helped bring this project to its current state of development, including the U.S. Department of Homeland Security (DHS), National Protection and Programs Directorate, Office of Infrastructure Protection, Protective Security Coordination Division management team, which consisted of Derek Mathews, Donald Robinson, and former DHS Protective Security Advisor (PSA) supervisor Louis Dabdoub. Their leadership and dedication inspired the Argonne National Laboratory team. Many other PSAs also contributed. In particular, the authors wish to acknowledge Billy Sasser, Max Fenn, Buck Hamilton, and James Hardy for their contributions during many late night working group meetings. The authors also thank several of their Argonne colleagues who contributed to the methodology and weighting process, including Stephen Folga, Michael McLamore, Shabbir Shamsuddin, Tracy Rager, and Tracie Hanson. In addition, Karen Guziel, John DePue, and Margaret Clemmons performed a thorough and thoughtful edit and review of the document. Finally, special thanks go to Mike Norman at DHS, who had the vision to evolve the Enhanced Critical Infrastructure Protection (ECIP) Program into its current state, and to Sean McAraw, who is the current ECIP project manager and continues to enhance the program.

This page intentionally blank

Executive Summary

The U.S. Department of Homeland Security (DHS) has directed its Protective Security Advisors (PSAs) to form partnerships with the owners and operators of the Nation's critical infrastructure and key resources (CIKR) and to conduct site visits for these assets as part of the Enhanced Critical Infrastructure Protection (ECIP) Program. During each site visit, a PSA uses the Infrastructure Survey Tool (IST) to document information on the facility's current CIKR protection posture and overall security awareness. The IST has more than 1,500 variables covering 6 major components (e.g., physical security) and 42 subcomponents (e.g., access control).

To optimize the use of this rich data source and to facilitate comparisons among critical assets across sectors, a procedure has been developed to use the collected data to estimate a Vulnerability Index (VI). The process for developing a VI begins with development of a Protective Measures Index (PMI). The PMI has a constructive sense in that it increases (gets better) as protective measures are added. The information is being used to assist DHS in analyzing sector and subsector vulnerabilities, to identify potential ways to reduce vulnerabilities, and to assist in preparing sector risk estimates. The owner/operator also receives an analysis of the data collected for a specific asset, which shows a comparison between the facility's protection posture and that of other DHS sector/subsector sites visited. This comparison gives the owner/operator an indication of the asset's security strengths and weaknesses that may be contributing factors to its vulnerability and protection posture.

The PMI ranges from 0 (low protection) to 100 (high protection). The index is based on the variables measured in the IST and indicates the particular asset's level of vulnerability (low vulnerability for low VI values and high vulnerability for high VI values). The PMI is converted to a VI by using the formula, 100 – PMI. Thus, low VI values indicate greater levels of protection than high VI values. When the owner/operator adds a protective measure, the value of the VI decreases and the PMI increases.

Figure ES-1 illustrates one way to display the results of an ECIP/IST analysis to the owner/operator of an asset. The PMI scale ranges from 0 (most vulnerable, as indicated by the measures included in the ECIP/IST) to 100 (least vulnerable). The PMI value for the particular asset being assessed is labeled "Your Asset." The lowest and highest PMI results for similar assets within the sector and the sector average are included to show how the current asset compares to other assets in the sector.

The development of the PMI and the associated VI is intended to assist DHS in conducting analyses of the vulnerabilities associated with the Nation's CIKR and to explore cost-effective ways to reduce those vulnerabilities. In addition, the approach can provide (1) valuable information to the owners and operators about where they stand relative to similar U.S. assets and (2) protective measures that they may want to consider that will reduce their vulnerability. The applications and uses of the PMI are at a very early stage in the ECIP Program, and improvements in concept and approach are expected as the program matures.

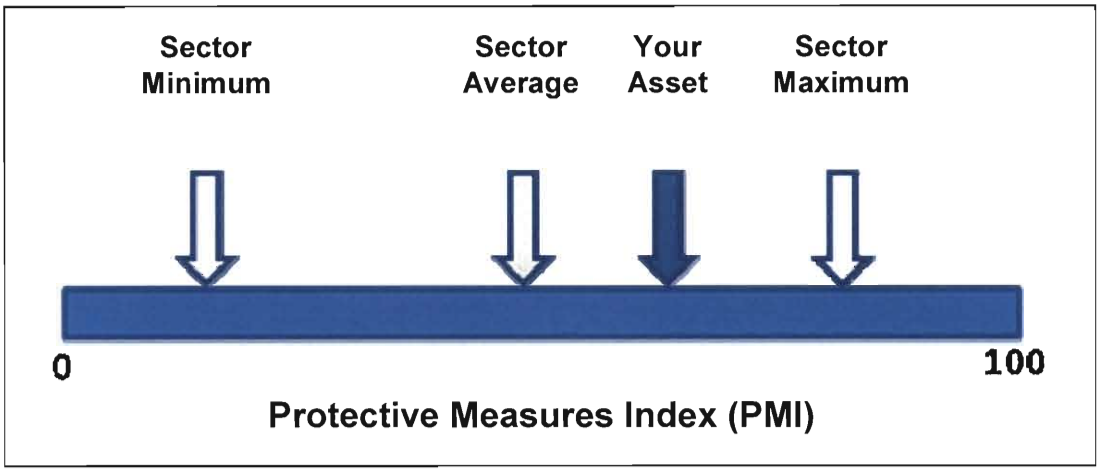

Figure ES-1: One Option for Displaying Results of ECIP/IST Analysis to Asset Owner/Operator

1 Introduction

The U.S. Department of Homeland Security (DHS) has directed its Protective Security Advisors (PSAs) to form partnerships with the owners and operators of assets most essential to the Nation's well being – a subclass of critical infrastructure and key resources (CIKR) – and to conduct site visits for these and other high-risk assets as part of the Enhanced Critical Infrastructure Protection (ECIP) Program. During each such visit, the PSA documents information about the facility's current CIKR protection posture and overall security awareness. The primary goals for ECIP site visits (DHS 2009) are to:

- Inform facility owners and operators of the importance of their facilities as an identified high-priority CIKR and the need to be vigilant in light of the ever-present threat of terrorism;

- Identify protective measures currently in place at these facilities, provide comparisons of CIKR protection postures across like assets, and track the implementation of new protective measures; and

- Enhance existing relationships among facility owners and operators; DHS; and various Federal, State, local, tribal, and territorial partners.

PSAs conduct ECIP visits to assess overall site security; educate facility owners and operators about security; help owners and operators identify gaps and potential improvements; and promote communication and information sharing among facility owners and operators, DHS, State governments, and other security partners. Information collected during ECIP visits is used to develop metrics; conduct sector-by-sector and cross-sector vulnerability comparisons; identify security gaps and trends across CIKR sectors and subsectors; establish sector baseline security survey results; and track progress toward improving CIKR security through activities, programs, outreach, and training (Snyder 2009).

The data being collected 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 needs to be reproducible, support risk analysis, and go beyond protection. It also needs to address important security/vulnerability topics, such as physical security, cyber security, systems analysis, and dependencies and interdependencies.

This report provides an overview of the approach being developed to estimate vulnerability and provide vulnerability comparisons for sectors and subsectors. The information will be used to assist DHS in analyzing existing protective measures and vulnerabilities at facilities, to identify potential ways to reduce vulnerabilities, and to assist in preparing sector risk estimates. The owner/operator receives an analysis of the data collected for a specific asset, showing a comparison between the facility's protection posture/vulnerability index and those of DHS sector/subsector sites visited. This comparison gives the owner/operator an indication of the asset's security strengths and weaknesses that may be contributing factors to its vulnerability and protection posture. The information provided to the owner/operator shows how the asset

compares to other similar assets within the asset's sector or subsector. A "dashboard" display is used to illustrate the results in a convenient format. The dashboard allows the owner/operator to analyze the implementation of additional protective measures and to illustrate how such actions would impact the asset's Protective Measures Index (PMI) or Vulnerability Index (VI).

2 The Infrastructure Survey Tool

The Infrastructure Survey Tool (IST) used by the PSAs for data input during ECIP site visits is designed to collect information in a more consistent manner with a more defined focus than was possible during earlier Site Assistance Visits. The IST is updated periodically to reflect PSA experience and to appropriately represent the characteristics of various vulnerability components. The IST is accessed online through the secure DHS LENS[1] system; it is also available in a hardcopy paper format.

The current version of the IST incorporates more than 1,500 variables covering 6 major components and 42 subcomponents (Table 1). Many of the subcomponents are quite detailed. For example, the building envelope subcomponent of physical security has seven contributing factors:

1. Standoff distance
2. Window characterization
3. Window alarms
4. Door security
5. Door alarms
6. Key control
7. Locks and containers

These factors have 48 data input values in the current version of the IST.

The IST includes additional information that is not used directly for calculating the PMI and VI. These items include general asset information, contact information for first preventers/responders and regulatory agencies, asset overview data (e.g., number of structures), criticality (e.g., asset replacement value), and the potential need for additional DHS products/services (e.g., training opportunities). The IST focuses on vulnerability information and not on threat and consequence information, although some high-level questions touch on these subjects.

[1] LENS is the Linking Encryption Network System, a portal that provides secure access to DHS documents.

Table 1: Major Components and Subcomponents for Measuring Vulnerability in the IST

Major Components and Subcomponents
1. Physical Security a. Access control b. Fences c. Gates d. Closed-circuit television (CCTV) e. Intrusion detection system (IDS) f. Parking g. Lighting h. Vehicle access control i. Building envelope
2. Security Management a. Business continuity plan b. Security plan c. Emergency action plan d. Threat levels e. Security information communication f. External security exercises g. Executive protection program h. Security working groups i. Sensitive information identified j. National security clearance k. Background checks
3. Security Force a. Staffing b. Equipment/weapons c. Training d. Post guidelines e. Patrols f. Random patrols g. After hour security h. Checks recorded i. Command and control j. Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA)
4. Information Sharing a. Threat sources b. Information sharing mechanisms
5. Protective Measures Assessment a. New protective measures b. Random security measures
6. Dependencies a. Critical products (chemicals, fuels, raw materials, packaging, medical supplies, feed, and by-products/wastes) b. Electricity c. Information technology (internal and Internet business, and internal and Internet control) d. Natural gas e. Telecommunications (telephone, data, and radio link) f. Transportation (rail, air, road, maritime, and pipeline) g. Water h. Wastewater

3 Estimating Vulnerability from the ECIP/IST Data

3.1 Compiling the Vulnerability Index

The IST provides asset- or facility-based information from a wide range of CIKR facilities, such as commercial buildings, electrical substations, and dams. The estimation of a single VI incorporates differing security postures for the 18 CIKR sectors (Table 2) and their associated subsectors. For example, fences are relatively important protective measures at electrical substations but in general are not important for commercial buildings. Subsector-level consideration is often important. For example, the Commercial Facilities Sector includes diverse subsectors, such as shopping malls and sports arenas, with very different security approaches.

Table 2: 18 Critical Infrastructure and Key Resources Sectors

No.	Sector
1	Banking and Finance
2	Chemical
3	Commercial Facilities
4	Communications
5	Critical Manufacturing
6	Dams
7	Defense Industrial Base
8	Emergency Services
9	Energy
10	Food and Agriculture
11	Government Facilities
12	Healthcare and Public Health
13	Information Technology
14	National Monuments and Icons
15	Nuclear Reactors, Materials, and Waste
16	Postal and Shipping
17	Transportation Systems
18	Water

Each of the six major IST components has a vulnerability that depends on the type of threat under consideration (such as those included in the Strategic Homeland Infrastructure Risk Assessment process) and the sector (or subsector). For example, one would expect vehicle access control to be a more important vulnerability factor for the threat of a vehicle-borne improvised explosive device (VBIED) than for the threat of an improvised explosive device (IED).

The VI ranges from 0 (low vulnerability) to 100 (high vulnerability). The index is intended to provide a summary value indicating an asset's vulnerability based on data in the IST. It is important to note that VI = 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 ECIP/IST 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.

Because the IST indicates whether protective measures, procedures, and policies have been implemented to reduce vulnerability, a more intuitive index would go from 0 to 100, with a higher index value – indicating a higher level of protection – being more desirable than a lower index value. This index is referred to as the overall PMI and is defined as:

$$PMI = 100 - VI, \quad (1)$$

where:

PMI = overall Protective Measures Index, ranging from 0 (high vulnerability as measured by the items included in the IST) to 100 (low vulnerability as measured by the items included in the IST); and

VI = Vulnerability Index, ranging from 0 (low vulnerability as measured by the items included in the IST) to 100 (high vulnerability).

The relationship between the VI and PMI is shown in Figure 1. When the VI is low, the PMI is high, and vice versa. When an action is taken to reduce vulnerability (move to the left along the horizontal axis), the VI goes down and the PMI goes up.

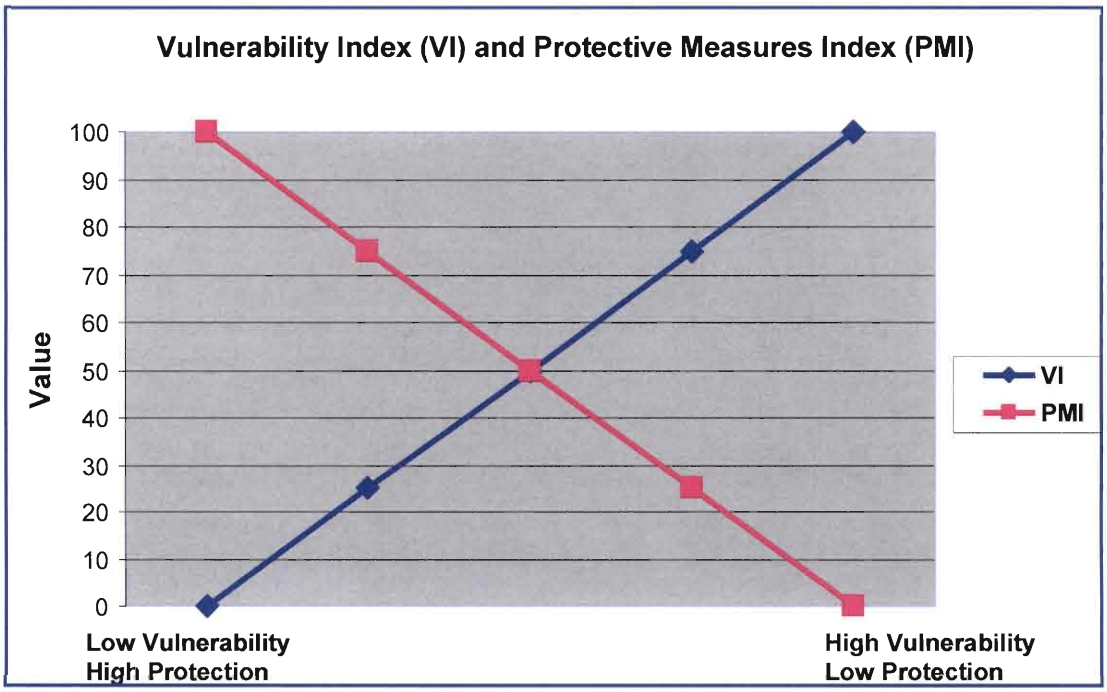

Figure 1: Relationship of Protective Measures Index to Vulnerability Index

3.2 Constructing the Protective Measures Index

The overall PMI consists of a weighted sum of six major components (Table 1), as shown in Equation 2:

$$\text{PMI} = \sum_{i=1}^{6} a_i \times X_i \tag{2}$$

where:

a_i = scaling constant (weight; a number between 0 and 1) indicating the relative importance of component i of PMI; and

X_i = value of component i of the PMI (e.g., physical security).

The six weights (a_i) in Equation 2 are called *Level 1 weights* and vary according to the sector (or subsector) and threat. The value of X_i is referred to as the PMI for component i (e.g., X_1 is the PMI for physical security).

The physical security PMI is a function of the nine subcomponents listed in Table 1 (e.g., access control, fences) and is estimated as the weighted sum in Equation 3:

$$\text{PSPMI} = \sum_{i=1}^{9} b_i \times Y_i \tag{3}$$

where:

PSPMI = PMI for physical security (ranging from 0 to 100);

b_i = scaling constant (weight) indicating the relative importance of component i of PSPMI; and

Y_i = value of component i of the PSPMI (e.g., access control).

The nine weights (b_i) in Equation 3 are called *Level 2 weights* and depend on the sector (or subsector) and threat. The value of Y_i is referred to as the PMI for subcomponent i (e.g., Y_1 is the PMI for access control).

Similar equations hold for PMIs for the other five components of overall PMI, namely, security management (SMPMI), security force (SFPMI), information sharing (ISPMI), protective measures assessment (PMAPMI), and dependencies (DPMI). The number of subcomponents varies as shown in Table 1. There are 42 Level 2 weights for every sector/threat combination.

The physical security PMI consists of nine subcomponents (Equation 3), each of which is an index value. For example, the access control PMI consists of a weighted sum of five

contributors, as shown in Equation 4. The five contributors are consolidated access point control, identification check process, card access control systems, mail screening, and suspicious package procedures, all of which have their own index values.

$$\text{ACPMI} = \sum_{i=1}^{5} c_i \times Z_i \tag{4}$$

where:

ACPMI = PMI for access control (ranging from 0 to 100);

c_i = scaling constant (weight) indicating the relative importance of component *i* of ACPMI; and

Z_i = value of component *i* of the ACPMI (e.g., card access control systems).

The weights (c_i) in Equation 4 are called *Level 3 weights* and are independent of the sector (or subsector) and the threat. That is, the PMIs for access control, fences, gates, etc., are fixed characteristics of the subcomponents, just as the height of an individual is a fixed characteristic. The importance of access control relative to the other eight components of physical security is determined by the weights in Equation 3, and the importance of physical security relative to the other five major components of the PMI is determined by the weights in Equation 2. If, for example, in the Commercial Facilities Sector, fences are relatively unimportant compared to access control, they can be assigned a low (possibly 0) weight. In an analogous situation involving human beings, the height of an individual may be unimportant – and would be assigned a low weight – compared to other characteristics if one were evaluating typing potential, but, if one were evaluating basketball potential, the height characteristic could be very important and could be assigned a high weight.

The value of Z_i in Equation 4 is obtained from an index ranging in value from 0 (most vulnerable) to 100 (least vulnerable) for each component. The components of access control (Z_i) are as follows:

1. Consolidated access point control (separate factors for visitors and employees),
2. Identification check process,
3. Card access control systems,
4. Mail screening, and
5. Suspicious package procedures.

Level 3 weights address considerations such as how the added protection of a brick and mortar fence compared with a mesh aluminum chain-link fence. The Level 3 judgments (more than 1,600) were obtained from a group of subject-matter experts, consisting primarily of PSAs, and are fixed for all evaluations. Level 2 weights (e.g., that address the importance of access control compared to fences) and Level 1 weights (e.g., that address the importance of physical security

compared to security management) were obtained from subject-matter experts from each sector. The Level 1 and 2 weights depend on sector and threat.

Figure 2 provides an example calculation of the fence PMI for two different fences. The fence on the left is a 7-foot-high standard aluminum chain-link fence with 45-degree outriggers, barbed wire, anchored base, and a clear zone (i.e., free of objects). This fence has a PMI of 60 (100 is the highest PMI and lowest vulnerability based on characteristics addressed in the IST). The fence on the right in Figure 2 is a 6-foot-high wood fence with a partial clear zone. This fence has a PMI of 13. The PMI results shown in Figure 2 indicate that the chain-link fence is significantly less vulnerable than the wood fence. Because these results are computed using Level 3 weights, they would be constant over all sectors and threats. Whether fences are important within the physical security PMI (Level 2 weight), and whether physical security PMI is important within the overall PMI (Level 1 weight), are sector and threat dependent and are not specified in this example.

Figure 2: Fence PMI for Two Types of Fences

This page intentionally blank

4 Reference Set of Weights

A complete reference set of Level 1, 2, and 3 weights was obtained (in quantitative terms) from an expert group, primarily comprised of PSAs. Their evaluations were obtained at several different times throughout 2008, as the components of the PMI were being developed in conjunction with IST modifications to (1) address topics of concern within the ECIP Program and (2) leverage PSA experience in the field to increase the efficiency and effectiveness of the assessment process.

The weights were obtained in accordance with the principles of decision analysis (Keeney 1992; Keeney and Raiffa 1976). The weights for a set of components depend on the ranges (worst to best) as included in the IST. Preferences have been obtained over many specific values within the ranges of single components (e.g., preferences were obtained specifically for fence heights of 5 feet or less; 6, 7, and 15 feet; and greater than 15 feet). Conditions suitable for linear additive functions are assumed to hold for all PMI calculations. Sensitivity analysis to date indicates that this assumption is reasonable.

Level 1 and Level 2 weights were obtained for several sectors and subsectors over several relevant threat categories. In some cases, weights obtained from DHS sector experts from the Homeland Infrastructure Threat and Risk Analysis Center were initially used pending those to be obtained from sector representatives. Each sector assessment includes specification of appropriate subsectors[2] 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, IED, and VBIED threats. Sector representatives could specify additional threats deemed relevant either for the sector as a whole or for specific subsectors.

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, such as those listed above, are used. To establish that the set of weights obtained from the PSA group is reasonable, judgments about all three levels 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.

[2] 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 Systems 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).

This page intentionally blank

5 Illustrative Protective Measures Index

A PMI value considered in isolation is difficult to interpret; for example, a PMI of 50 does not necessarily correspond to an "average" rating. One of the primary benefits of the PMI scoring process is that it allows comparison across similar facilities within a sector or subsector or, possibly, across sectors. This comparison can be performed at Level 1, 2, or 3. The comparisons help to identify protective measures that may be considered for implementation at specific facilities.

Table 3 illustrates the calculation of a physical security PMI (PSPMI). The nine component PMIs for the illustrative asset are shown along with their Level 2 component weights (which sum to 1.0). The component weights are established by the PSA experts for a general threat and sector. Access control has the highest component weight (0.148), but it is less than twice the lowest component weight (0.082 for closed-circuit television [CCTV] and parking). These weights indicate that all nine components are significant in the calculation of physical security PMI. Multiplying the component weights and the component PMIs, as shown in Equation 3, yields the "weighted PMIs" shown in the last column in Table 3. Summing these values yields a PSPMI of 56.95. (Several numerical digits are shown to allow readers to follow the arithmetic, if desired.)

Table 3: Physical Security PMI for a General Threat (Illustrative Asset)

Physical Security Components	Level 2 Component Weights	Component PMIs	Weighted PMIs
Fences	0.116	39.36	4.57
Gates	0.134	45.71	6.13
CCTV	0.082	67.10	5.50
IDS	0.100	64.38	6.44
Parking	0.082	51.44	4.22
Access control	0.148	76.88	11.38
Lighting	0.110	83.67	9.20
Vehicle access control	0.128	44.33	5.67
Building envelope	0.100	38.40	3.84
	Σ = 1.000		
Physical Security Protective Measures Index		PSPMI=	56.95

Note: High values of PSPMI (range 0 -100) correspond to low vulnerability.

Table 4 illustrates the calculation of a security management PMI (SMPMI) for an illustrative asset. The 11 component PMIs are shown along with their Level 2 component weights. In this case, the highest component weights (security plan and background checks [0.120 each]) are more than twice the lowest (national security clearance [0.048]).

Table 4: Security Management PMI for a General Threat

Security Management Components	Level 2 Component Weights	Component PMIs	Weighted PMIs
Business continuity plan	0.108	49.82	5.38
Security plan	0.120	40.00	4.80
Emergency action plan	0.108	52.24	5.64
Threat levels	0.090	100.00	9.00
Security information communication	0.090	12.12	1.09
External security exercises	0.078	0.00	0.00
Executive protection program	0.058	0.00	0.00
Security working groups	0.072	0.00	0.00
Sensitive information identified	0.108	50.71	5.48
National security clearance	0.048	0.00	0.00
Background checks	0.120	25.00	3.00
	S = 1.000		
Security Management Protective Measures Index		SMPMI=	34.39

Note: High values of SMPMI (range 0 -100) correspond to low vulnerability.

Table 5 illustrates the calculation of a security force PMI (SFPMI). The 10 component PMIs are shown along with their Level 2 component weights. In this case, staffing is the component with the highest weight. (In the IST, staffing refers to adequacy of staffing across seven factors, such as physical complexity/size of the facility.) Staffing is considered to be very important, and its weight of 0.500 means this component is as important as the other nine components combined. The most important component of the other nine (training [0.070]) is approximately twice as important as the component with lowest weight (checks recorded [0.037]).

Table 6 illustrates the calculation of an information sharing PMI (ISPMI). In this case, there are only two components. They refer to how threat information is obtained and what mechanisms are used to share information. They are approximately equally weighted in the example.

Table 5: Security Force PMI for a General Threat

Security Force Components	Level 2 Component Weights	Component PMIs	Weighted PMIs
Staffing	0.500	92.50	46.25
Equipment/Weapons	0.059	61.86	3.65
Training	0.070	56.91	3.98
Post guidelines	0.049	100.00	4.90
Patrols	0.059	100.00	5.90
Random patrols	0.059	0.00	0.00
After hour security	0.059	0.00	0.00
Checks recorded	0.037	0.00	0.00
Command and control	0.059	100.00	5.90
MOU/MOA	0.049	0.00	0.00
	Σ = 1.000		
Security Force Protective Measures Index		SFPMI=	70.58

Note: High values of SFPMI (range 0 -100) correspond to low vulnerability.

Table 6: Information Sharing PMI for a General Threat

Information Sharing Components	Level 2 Component Weights	Component PMIs	Weighted PMIs
Threat	0.474	45.65	21.64
Information sharing mechanisms	0.526	52.15	27.43
	Σ = 1.000		
Information Sharing PMI		ISPMI=	49.07

Note: High values of ISPMI (range 0 -100) correspond to low vulnerability.

Table 7 illustrates the calculation of a protective measures assessment PMI (PMAPMI). Once again, there are only two components. In this case, they refer to whether new protective measures have been implemented within the past year and whether random security measures are used. They are approximately equally weighted in the example.

Table 8 illustrates the calculation of a dependencies PMI (DPMI). The eight component PMIs are shown along with their Level 2 component weights. In this case, all Level 2 weights were assumed to be equal. This assumption is reasonable for the general threat because no sector is identified.

Table 7: Protective Measures Assessment PMI for a General Threat

Protective Measures Assessment Components	Component Weights	Component PMIs	Weighted PMIs
New protective measures	0.556	60.00	33.36
Random security measures	0.444	46.15	20.49
	S = 1.000		
Protective Measures Assessment PMI		PMAPMI=	53.85

Note: High values of PMAPMI (range 0 -100) correspond to low vulnerability.

Table 8: Dependencies PMI for a General Threat

Dependencies Components	Level 2 Component Weights	Component PMIs	Weighted PMIs
Critical products	0.125	80.31	10.04
Electric	0.125	53.32	6.66
Information technology	0.125	42.77	5.35
Natural gas	0.125	53.97	6.75
Telecommunications	0.125	60.43	7.55
Transportation	0.125	43.29	5.41
Water	0.125	66.87	8.36
Wastewater	0.125	60.54	7.57
	Σ = 1.000		
Dependencies PMI		DPMI=	57.69

Note: High values of DPMI (range 0 -100) correspond to low vulnerability.

Table 9 illustrates the calculation of an overall PMI. The six major component PMIs, from Tables 3 through 8, are shown along with their Level 1 component weights. The illustrative Level 1 weights obtained from the PSA experts for the general threat show that the security management component was considered the most important (0.242), although three other major components were nearly equal in importance (physical security [0.215], security force [0.194], and dependencies [0.206]). The other two major components, information sharing and protective measures assessment (which cover significantly less subject matter in the IST than the other four major components), are considered less important. The overall PMI for the illustrative asset is 53.46, which corresponds to a VI of 46.54.

Table 9: Overall PMI for a General Threat

Vulnerability Index Components	Level 1 Component Weights (w_i)	Protective Measures Indexes (PMI_i)	Weighted PMI_i (w_i x PMI_i)
Physical Security (PSPMI)	0.215	56.95	12.24
Security Management (SMPMI)	0.242	34.39	8.32
Security Force (SFPMI)	0.194	70.58	13.69
Information Sharing (ISPMI)	0.080	49.07	3.93
Protective Measures (PMAPMI)	0.063	53.85	3.39
Dependencies (DPMI)	0.206	57.69	11.88
Overall Protective Measures Index (PMI*)		PMI*=	53.46
Overall Vulnerability Index (VI)		VI=100-PMI*=	46.54

Notes: (1) $PMI^* = \sum (w_i \times PMI_i)$; (2) high values of PMI* correspond to low vulnerability; (3) low values of VI correspond to low vulnerability.

This page intentionally blank

6 Sector and Threat Dependence of the Weights

Weights for Levels 1 and 2 depend on sector, or subsector, and threat. The weights obtained to date from the sectors and the PSAs have verified this fact. Table 10 shows the physical security component weights (Level 2 weights) obtained from the PSA group for general, IED, and VBIED threats. While access control was the most important component for general and IED threats, vehicle access control was the most important for VBIED threat. Also notable is that intrusion detection systems (IDSs) are more important for general and IED threats than for VBIED threat, and that parking is more important for VBIED threat than for general and IED threats.

Table 10: PSA Physical Security Component Weights as a Function of Threat

Physical Security Components	Level 2 Component Weights		
	General Threat	IED	VBIED
Fences	0.116	0.135	0.123
Gates	0.134	0.135	0.133
CCTV	0.082	0.076	0.082
IDS	0.100	0.111	0.073
Parking	0.082	0.078	0.130
Access control	0.148	0.148	0.116
Lighting	0.110	0.101	0.101
Vehicle access control	0.128	0.115	0.144
Building envelope	0.100	0.101	0.098

Table 11 indicates that the physical security component weights (Level 2 weights) for the VBIED threat are also a function of sector. Vehicle access control remains an important component for the General, Commercial Facilities, and Chemical Sectors, but it is less important than parking for the Commercial Facilities Sector. Fences and gates are significantly more important for the Chemical Sector than for the Commercial Facilities Sector. On the other hand, CCTV is much more important for the Commercial Facilities Sector than for the Chemical Sector. These results for the PSA group demonstrate that physical security Level 2 weights depend on sector and threat, as expected.

Table 11: PSA Physical Security Component Weights as a Function of Sector

Physical Security Components	Level 2 Component Weights		
	VBIED - General Sector	VBIED - Commercial	VBIED - Chemical
Fences	0.123	0.044	0.116
Gates	0.133	0.054	0.133
CCTV	0.082	0.141	0.066
IDS	0.073	0.091	0.084
Parking	0.130	0.163	0.132
Access control	0.116	0.127	0.124
Lighting	0.101	0.114	0.108
Vehicle access control	0.144	0.155	0.141
Building envelope	0.098	0.111	0.096

To date, Level 1 weights in general have not shown a strong dependence 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 Sectors. However, for the Healthcare and Public Health (HPH) Sector, six subsectors were defined, and Level 1 weights did vary somewhat over the seven threat categories examined. In a few instances for HPH, a strong dependence 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 HPH subsectors, but, for the mass fatality facilities subsector, security force had the lowest weight of the six major components (less than 6 percent of the total weight for the overall PMI).

This page intentionally blank

7 Comparison of Assets Using the PMI

The ECIP/IST results are not intended to serve as "the final word" for vulnerability. The ECIP/IST results are but one factor that can be considered in conjunction with many other factors. For example, a facility may have a very low PMI, but would have no reason to increase its PMI because there is no crime, no history of credible threat against the facility, or relatively insignificant consequence if the facility were attacked. Furthermore, 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 is not a vulnerability assessment or a risk assessment. It is a basic data collection tool most similar to a security survey. However, if the groupings for asset comparisons are selected appropriately, comparisons among assets may be informative and may help to identify areas for more in-depth analysis of potential improvements.

As mentioned earlier, a PMI value for a single asset is difficult to interpret. It does become meaningful when compared within a set of similar assets. It is assumed that a lower PMI value indicates greater vulnerability than a higher PMI value. Providing the owner/operator of an asset with a detailed analysis of its PMI and a comparison across other similar (but unnamed) assets is useful because it gives perspective as to where the subject asset stands relative to its peer group. The comparison can be at the highest level (overall PMI, Level 1), at the next highest level (e.g., physical security PMI, Level 2), or at numerous lower levels (e.g., access control PMI, Level 3, or mail screening, also Level 3, etc.). The lower-level comparisons provide good starting points for the owner/operator in considering which protective measures may be worthwhile additions. The higher-level comparisons provide a good indication of how the overall security posture at the asset compares within its peer group.

The most useful ways in which the information can be provided to the owner/operator are being improved as ECIP/IST experience increases. Two options are shown in Figures 3 and 4.

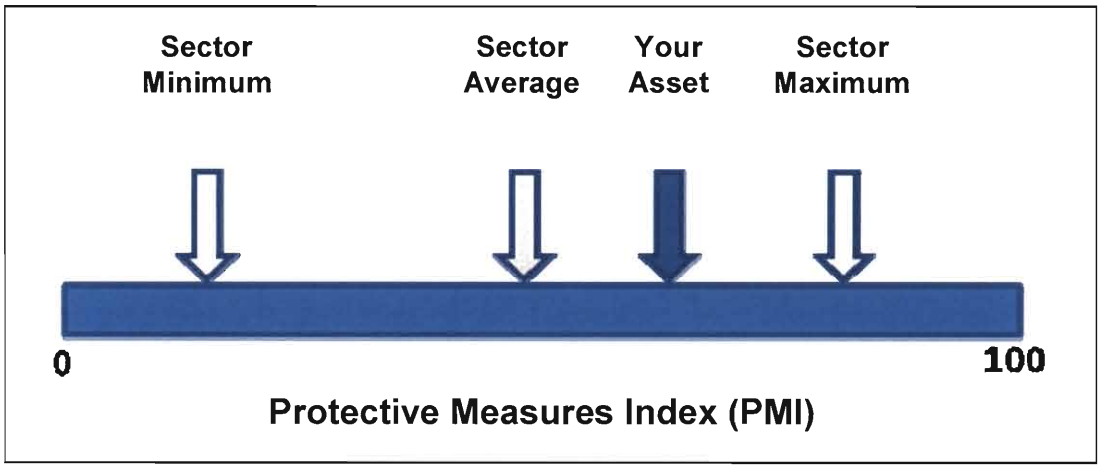

Figure 3: One Option for Displaying Results of ECIP/IST Analysis to Asset Owner/Operator

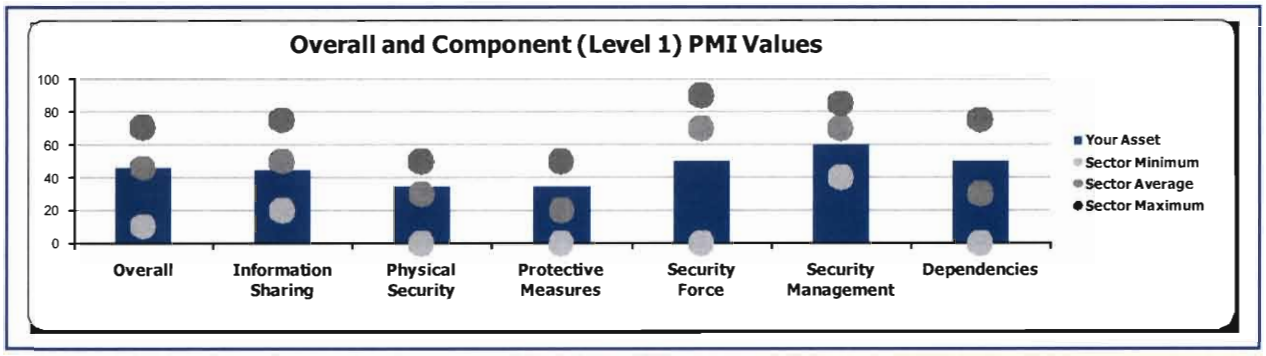

Figure 4: Display Option Showing PMI Values Compared to Sector Average Values

As shown in Figure 3, the entire PMI scale ranges from 0 (most vulnerable as indicated by the measures included in the ECIP/IST) to 100 (least vulnerable). In the figure, the PMI value of the asset for which the current assessment is being provided to the owner/operator is labeled "Your Asset." The lowest and highest PMI values for similar assets within the sector are shown along with the sector average. Such a display is not intended to imply that if an asset's PMI is greater than the sector average, there is no need to consider additional protective measures.

Displays such as Figure 3 can be prepared for the entire spectrum of measures included in the IST and levels included in the PMI calculations. For example, comparisons can be made of the height of the fence, the fence PMI, the physical security PMI, and the overall PMI.

Figure 4 shows a display option that includes an overall PMI and the six Level 1 components. The sector maximum, average, and minimum values are shown as dots, and the result for the facility receiving the summary is labeled "Your Asset." This type of chart can be prepared for all three levels of information available from the ECIP/IST data. An advantage of comparisons such as shown in Figure 4 is that they draw attention immediately to components that are well below the sector average, such as security force in Figure 4. The owner/operator may wish to examine reasons for this difference and consider ways to reduce vulnerability. A disadvantage of comparisons such as shown in Figure 4 is that they can give the mistaken impression that sector average values are indicative of desired or adequate performance.

Collecting the ECIP data and comparing the sector average PMI can provide DHS with useful insights. For example, a recent analysis of 349 assets (Figure 5) showed that the security force PMIs for the Banking and Finance, Defense Industrial Base, Commercial Facilities, and Government Facilities Sectors were relatively high (65–83), whereas the security force PMIs for the Emergency Services, Dams, Energy, Transportation Systems, and Healthcare and Public Health Sectors were relatively low (30–38).

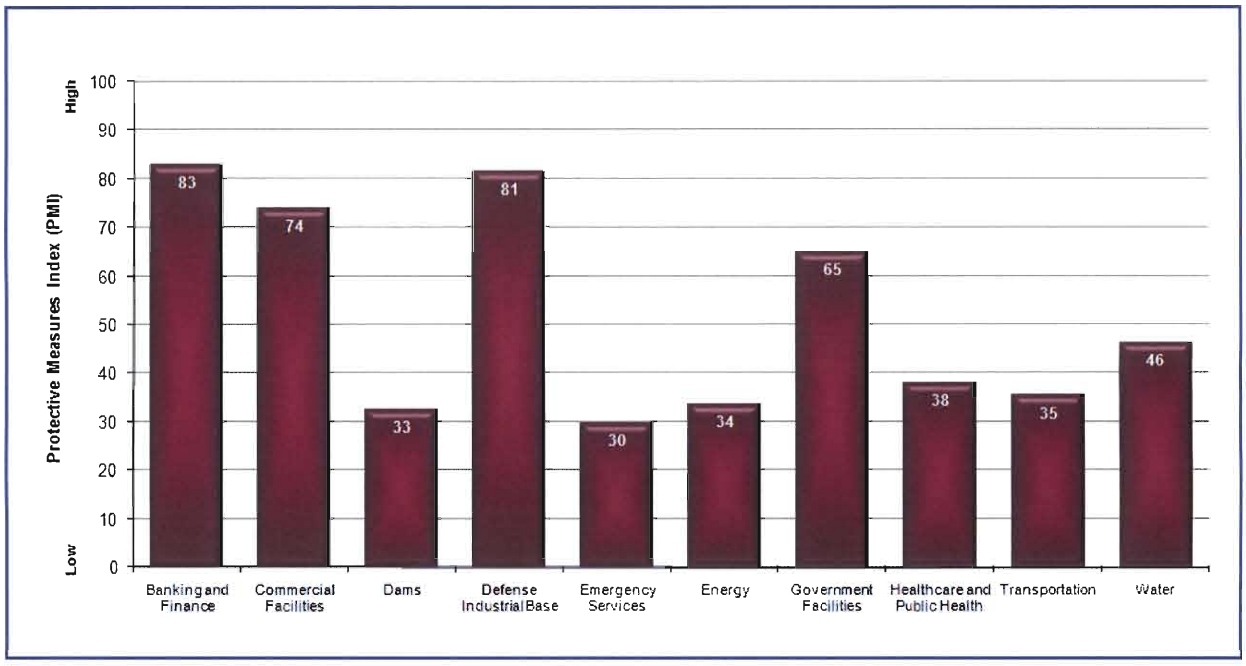

Figure 5: Illustrative Analysis of Security Force PMI by Sector

An examination of these results at a more detailed level highlights the need for subsector analysis to put asset comparisons in proper perspective for some sectors, depending on sector homogeneity. For example, the 53 Energy Sector assets had an average security force PMI of 34. Further inspection showed that less than half of the assets had a security force. However, major refineries and electricity control centers are examples of Energy Sector assets that were likely to have security force PMI of 80 or more. Therefore, it appears that Energy Sector comparisons provided to owners/operators should reflect at least two or more different subsectors.

Although the IST is a data collection tool and PSAs do not specifically identify gaps or provide options for consideration within the ECIP/IST, the IST data do provide value judgments that allow owners/operators to use the information provided after an ECIP visit to identify their own gaps (e.g., a fence index that is far below the average for similar facilities within their sector). They can also use this information to help identify protective measures that will improve their PMI (and conversely lower their VI).

Facility-specific PMIs essentially demonstrate the effects of management decisions concerning the prioritization of protective measures for a particular facility. The list of common security options identified through comparison with other similar facilities is intended to assist security managers in making decisions regarding a site-specific security strategy. No two facilities are alike, and, therefore, each facility's security staff and management team must determine the appropriate combination of protective measures on the basis of its own assessment of risks, taking into consideration threat, specific assets to be protected, consequences, overall vulnerability, facility characteristics, business impacts, and return on investment. The information from the ECIP/IST provides consistent insight into elements of vulnerability and consequence that can aid in the overall analysis.

8 Conclusion

The development of the Protective Measures Index and the associated Vulnerability Index is intended to assist DHS in conducting analyses of the vulnerabilities associated with the Nation's CIKR and identifying potential ways to reduce them. In addition, the approach can provide valuable information to facility owners and operators about their standing relative to similar sector assets and ways to reduce vulnerability. The applications and uses of the PMI and the VI for the ECIP Program continue to evolve, and improvements in concept and additional enhancements and approaches are expected as the program matures.

This page intentionally blank

9 References

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

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

Snyder, James 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 October 5, 2009).

U.S. Department of Homeland Security, 2009, *National Infrastructure Protection Plan: Partnering to Enhance Protection and Resiliency*; available at http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf (accessed October 5, 2009).

This page intentionally blank

10 Acronyms

CCTV	Closed-Circuit Television
CIKR	Critical Infrastructure and Key Resources
DHS	U.S. Department of Homeland Security
ECIP	Enhanced Critical Infrastructure Protection
HPH	Healthcare and Public Health
IDS	Intrusion Detection System
IED	Improvised Explosive Device
IST	Infrastructure Survey Tool
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
NIPP	National Infrastructure Protection Plan
PMI	Protective Measures Index
PSA	Protective Security Advisor
VBIED	Vehicle-Borne Improvised Explosive Device
VI	Vulnerability Index

Decision and Information Sciences Division
Argonne National Laboratory
9700 South Cass Avenue, Bldg. 900
Argonne, IL 60439-4867

www.anl.gov