ANL/GSS-17/2

Cyber Protection and Resilience Index: An Indicator of an Organization's Cyber Protection and Resilience Program

Global Security Sciences Division

ANL/GSS-17/2

Cyber Protection and Resilience Index: An Indicator of an Organization's Cyber Protection and Resilience Program

by
A.L. Joyce, F.D. Petit, J.A. Phillips, L.B. Nowak, and N.J. Evans
Global Security Sciences Division, Argonne National Laboratory

October 2017

1 Contents

List of Tables ii
List of Figures ii
List of Abbreviations iii
Acknowledgments iv
Executive Summary v
1 Introduction 1
2 Objectives 3
3 Multi-Attribute Decision Analysis 7
4 Implementation 9
4.1 Identifying Program Attributes 10
4.2 Determining Weights for Attributes 17
4.3 Data Collection 18
4.4 Visualization Tool 19
5 Methodology Advantages and Limitations 23
6 Future Developments 25
7 Conclusion 27
8 References 29
Appendix: CPRI Level Breakdown 31

List of Tables

Table 1. Comparison between CPRI Level 1 and NIST Functions 11
Table 2. CPRI Level 2 – Cybersecurity Management Subcomponents Description 13
Table 3. CPRI Level 2 – Cybersecurity Forces Subcomponents Description 14
Table 4. CPRI Level 2 – Cybersecurity Controls Subcomponents Description 15
Table 5. CPRI Level 2 – Incident Response Subcomponents Description 16
Table 6. CPRI Level 2 – Cyber Dependencies Subcomponents Description 16

List of Figures

Figure 1. CSET Tool Sample Results 4
Figure 2. Value Tree 7
Figure 3. Cyber Protection and Resilience Index – Level 1 Components 11
Figure 4. Cybersecurity Management – Level 2 Subcomponents 12
Figure 5. Cybersecurity Forces – Level 2 Subcomponents 13
Figure 6. Cybersecurity Controls – Level 2 Subcomponents 14
Figure 7. Incident Response – Level 2 Subcomponents 15
Figure 8. Cyber Dependencies – Level 2 Subcomponents 16
Figure 9: Illustrative Screenshot of the CPRI Dashboard 20
Figure 10: CPRI Training Scenario 21

List of Abbreviations

Argonne	Argonne National Laboratory
CCS	Critical Cyber Service
CFATS	Chemical Facility Anti-Terrorism Standards
CI	Critical Infrastructure
C-IST	Cyber Infrastructure Survey Tool
CPRI	Cyber Protection Resilience Index
CSA	Cyber Security Advisor
CSET	Cyber Security Evaluation Tool
CS&C	Cybersecurity and Communications
DDoS	Distributed Denial of Service
DHS	U.S. Department of Homeland Security
DoD	U.S. Department of Defense
DoS	Denial of Service
EO	Executive Order
GSS	Global Security Sciences
ISO	International Organization for Standardization
IT	Information Technology
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
QA	Quality Assurance
RISC	Risk and Infrastructure Science Center
SAL	Security Assurance Level
SLTT	State, Local, Tribal, and Territorial
SME	Subject Matter Expert

Acknowledgments

The authors gratefully acknowledge the contributions of many people who helped bring this project to its current state of development, including the management team of the U.S. Department of Homeland Security's (DHS's) Office of Cybersecurity and Communications. The authors are particularly thankful to the subject matter experts from the industry, DHS Cyber Security Advisors, State, Local, Tribal, and Territorial (SLTT) Governments, and National Laboratories that participated in the elicitation process; and other Argonne colleagues who made this report possible.

The authors also wish to thank the following members of the Argonne Analysis Team for their significant contributions: Dr. William Buehring, Dr. Ronald Whitfield, and Ms. Angeli Tompkins.

Executive Summary

In 2014, the U.S. Department of Homeland Security (DHS) and its Cyber Security Advisors (CSAs) began surveying critical infrastructure by using the Cyber Infrastructure Survey Tool (C-IST). The collected information is specific to an organization's cyber protection and resilience program on a critical cyber service (CCS), which includes management, personnel, controls, incident response, and cyber dependencies. Each of these areas contains options with varying cost and effectiveness, and owners and operators of critical infrastructure require a means of evaluating their existing protection and resilience systems against those alternative options. Evaluations must provide a quantitative metric that represents the expected overall effectiveness of the complete system and allows organizations' decision makers to pursue the strengthening of their programs. As a result, the Argonne National Laboratory Global Security Sciences (GSS) Division's Risk and Infrastructure Science Center (RISC) has developed such a metric, the Cyber Protection Resilience Index (CPRI), which serves to evaluate the effectiveness of an organization's cyber protection and resilience program. The structure of the CPRI is consistent with the functions as defined in the National Institute of Standards and Technology (NIST) Framework for Improving Critical Infrastructure Cybersecurity.

The index takes into account the diverse nature of protection and resilience programs by recognizing the relative importance or effectiveness of the various attributes that compose a program through assigning relative weights to each attribute. Relative weights are obtained by systematic elicitation of cybersecurity subject matter experts and used to calculate the CPRI. The CPRI value reflects the overall level of protection and resilience that is afforded by existing or anticipated cybersecurity programs. The CPRI ranges from 0 (low protection and resilience) to 100 (high protection and resilience).

A survey is administered by a trained individual by performing an inventory of a facility's cybersecurity program as it relates to a CCS and determining its current controls and response measures. The tool then applies the established relative weights to collected responses to calculate the composite index, which provides an indication of the expected overall program effectiveness relative to similar CCSs within the sector. In addition to the overall index, component indices are calculated for key categories of protection and resilience programs.

The CPRI Dashboard presents the overall CPRI and five subcomponent indices, along with the comparison to the high, median, and low values recorded for similar CCS types. The interactive dashboard can then be used to perform scenario analyses on hypothetical program modifications. As the number of completed surveys expands, the CPRI Dashboard narrows its comparison values only to surveys with similar CCSs within a specific sector, thereby improving the accuracy of the results. The CPRI methodology has been developed for use by all 16 critical infrastructure sectors (DHS, 2015a) for benchmarking and improvement.

This page intentionally left blank.

1 Introduction

In February of 2013, Executive Order (EO) 13636, *Improving Critical Infrastructure Cybersecurity*, emphasized the need to develop and implement collaborative risk management approaches to cybersecurity. EO 13636 recognizes that risks to critical infrastructure (CI) from cyber intrusions and unidentified cybersecurity vulnerabilities are a national security challenge that needs to be mitigated (U.S. President, 2013). In February of 2014, the National Institute of Standards and Technology (NIST) issued the *Framework for Improving Critical Infrastructure Cybersecurity* (NIST, 2014). This framework defines five core functions for improving the protection and resilience of CI: identification, protection, detection, response, and recovery.

A cyber protection and resilience program typically involves management, training, enforcement, controls, and incident response. Each of these areas contain options selected from multiple alternatives of varying cost and effectiveness. Owners and operators of CI must evaluate their existing protection and resilience systems against those alternative options that will ideally provide a quantitative metric that represents the expected overall effectiveness of the complete system. While there is no absolute scale for such an evaluation, a relative metric that identifies the effectiveness of a specific system in the context of systems for like organizations would provide a useful perspective. Decision makers in organizations that have relatively weak protection or that appear to have relatively poor resilience, as indicated by the metric, may use it to justify strengthening their programs and selecting alternative or alternative controls.

Argonne National Laboratory's (Argonne's) Global Security Sciences (GSS) Division's Risk and Infrastructure Science Center (RISC), in collaboration with the U.S. Department of Homeland Security (DHS) Office of Cybersecurity and Communications (CS&C), has developed a composite measure, the Cyber Protection Resilience Index (CPRI), which is intended to serve as an indicator of the effectiveness of an organization's cyber protection and resilience programs as it relates to a critical cyber service (CCS), and to allow organizations to compare cybersecurity information among similar organizations within the sector. The approach takes into account the diverse nature of cyber protection and resilience programs and uses the principle of multi-criteria decision analysis in creating an index ranging from 0 to 100.

This report provides an overview of the approach that was developed to estimate the cyber protection and resilience of CI systems. The information is used to assist DHS and CI owners and operators in analyzing existing capabilities and programs and in identifying potential ways to increase protection and resilience. The provided information from the CPRI approach can then be used by CI owners and operators to understand how they compare to similar organizations and to help them make risk-based decisions. A "dashboard" display, which provides an interactive tool rather than a static report, presents the results of the CPRI in a convenient format and allows testing of different scenarios in order to model the influence of additional protection and resilience measures on the CI's CPRI.

This page intentionally left blank.

2 Objectives

Cybersecurity best practice guidelines and standards have been developed by NIST (NIST, 2005; NIST, 2011), the North American Electric Reliability Corporation (NERC) (NERC, 2006), DHS (CFATS, 2009, DHS, 2009), the U.S. Department of Defense (DoD) (DoD, 2003), and other organizations (ISO/IEC, 2009). According to these best practices and standards, the development of a cyber protection and resilience metric must address four principal challenges:

1. Programs for cyber protection and resilience are typically multi-dimensional. The effectiveness of various attributes for such a program are described in differing units because of the diverse nature of those attributes, thus making it difficult to obtain a combined effectiveness rating that characterizes an entire program.
2. Performance assessment for program elements is fundamentally subjective. Incorporating these assessments into a program evaluation requires the use of methods that can incorporate subjective as well as objective measures of performance.
3. Systematic characterization of the cyber protection and resilience program for a specific organization.
4. The evaluation mechanism must be able to represent current state and potential changes in cyber protection and resilience practices both flexibly and conveniently in order to evaluate opportunities to strengthen a program.

Prior work, performed in developing the DHS Cyber Security Evaluation Tool (CSET), has addressed the first and third of these challenges by providing a self-assessment survey for organizations to complete (DHS, 2015b). CSET, which can be installed on a desktop or laptop system, allows a user to perform a self-evaluation comparison to the selected standards. Based on this comparison and a desired Security Assurance Level (SAL), CSET produces a best-practices list and identifies current standard gaps. CSET uses the responses to questions about the consequences of a cyber-attack to calculate the SAL. The strengths of the CSET system include its direct reliance on specific standards, which can be selected by the facility user, and its recognition of consequences to establish a preferred level of protection. Figure 1 shows sample results from the CSET tool.

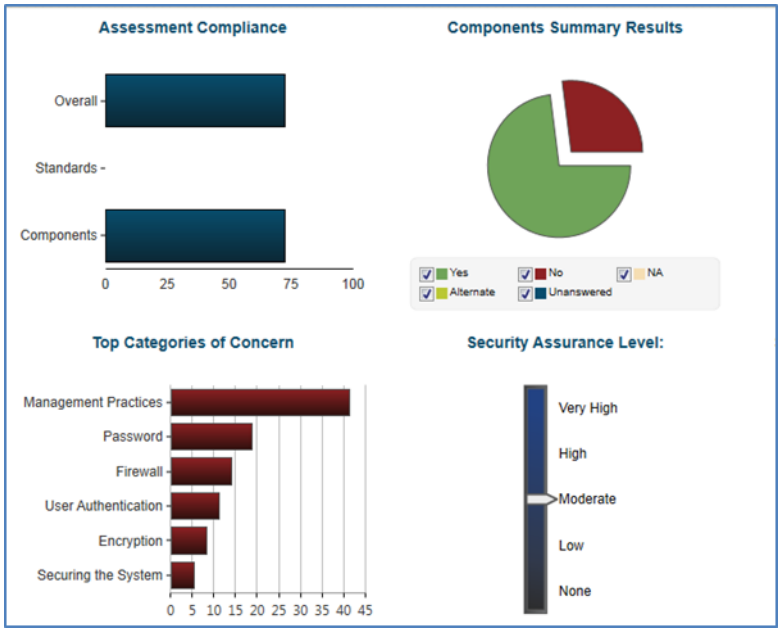


Figure 1. CSET Tool Sample Results

Rather than providing an overall assessment of the program as reported by the organization, CSET provides a comparison of the respondent's critical cyber service against well-known cybersecurity standards. CSET does not perform an overall program evaluation or provide a composite measure.

Other cyber protection and resilience assessments have been developed and can be categorized into two groups:

- Organization-specific, in which expert opinions are solicited and compiled for one organization; and
- Technology-specific, in which particular hardware, software, or organizational approaches to cybersecurity are evaluated.

The results of organization-specific assessments can be extended to other, very similar, organizations in the interest of establishing standards or regulations for that type of organization. The nuclear power industry is an example of organization-specific cybersecurity assessments evolving into regulatory requirements.

Technology-specific assessments generally use penetration testing for identifying deficient areas in both hardware and software. This type of assessment can possibly result in a modification of policy in the case of more widespread problems.

Similar to CSET, existing cyber protection and resilience assessment methodologies do not address all four challenges supporting the development of an aggregated cyber protection and resilience metric. As a result, Argonne's GSS Division's RISC has developed a composite measure, the CPRI. This aggregated index considers various attributes of a CI's cyber protection and resilience program in order to evaluate its effectiveness.

The development of the CPRI has four main objectives to address the challenges described above:

1. Organize protection and resilience attributes by category and allow scores to be combined across categories for each measure.
2. Address subjective evaluation by employing expert opinion to define the relative contribution of each attribute to the overall CI cyber protection and resilience.
3. Develop a survey tool that allows for a systematic inventory of a CI's cyber protection and resilience program elements and controls.
4. Develop an interactive display of the overall index and category indices, allowing a CI manager to evaluate program enhancements.

A multi-attribute decision analytic approach, described in Section 3, was used to reach these objectives. The developed methodology and its implementation are presented in Sections 4 and 5.

This page intentionally left blank.

3 Multi-Attribute Decision Analysis

The objective of multi-attribute decision analytic approach is to identify attributes with potentially disparate measures and transform them into a common metric to inform decisions. Identifying attributes relies on determining pertinent stakeholders that will make and/or be affected by those decision. Stakeholders may include those that are close to the evaluated program (e.g., decision makers, information technology [IT] administrators, managers, and operators) and individuals who are not directly influenced by the program but have an interest in the evaluation (e.g., sponsors, regulatory authorities, standards authorities, or academia).

The level of authority held by the decision maker(s) and the decision(s) to be informed drive the proper identification of stakeholders. For example, if the decision to be made determines the best portfolio of projects for a small component of a large agency whose impact would be limited to the component, the stakeholders would consist only of personnel with a direct relationship to that component. Alternatively, if the decision to be made resides at the organizational level, high-level members of that organization, as well as ranking members of other organizations that might be impacted, would be a more appropriate group of stakeholders to define the attributes.

As an aid to eliciting, culling, and refining attributes and to determining the final elicitation of weights, attributes can be organized in a hierarchical structure known as a value tree (Figure 2). The root node (*A*) of the tree is the objective of the evaluation. Intermediate nodes (*B*, *E*, *C*, and *G*) are categories into which attributes are intuitively organized. Several levels of category branches are possible. At the lowest level, or leaves of the tree, nodes (*D*, *F*, *I*, *H*, and *J*) are individual attributes. Weight values are assigned to each node of the tree to represent its relative importance, or contribution to the overall objective, and are then applied to the calculation of the index. In more formal terms, the index is a weighted linear aggregation of values that are associated with individual attributes.

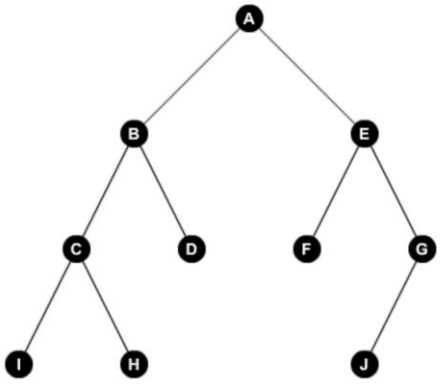


Figure 2. Value Tree

For the above tree, the following formula defines the value of the final objective A:

$$A = \sum_{i=1}^{2} w_i \, x_i$$

Equation 1. Weighted Linear Aggregation

where: *A* is the overall index;

w_i is the scaling constant (weight; a number between 0 and 1), indicating the relative importance of possibility i (i = 1,2) of *A*; and

x_i is the index value of component *i* of *A* (i.e.. nodes B and E).

This aggregation process results in an index that varies from 0 to 100, thus allowing for comparison and serving as a guide for decision-making.

4 Implementation

Making decisions using disparate sources of information has been an area of research for the decision analytic community for decades. The Value-Focused Thinking methodology (Keeney, 1992) used to construct the CPRI builds upon axioms and theories from multi-attribute utility theory (Keeney and Raiffa, 1976) to bring disparate factors together under a common metric to inform decisions.

The establishment of the attributes that will be used to construct the index value is a crucial first step. Experts can assist in the development of these attributes, given the ultimate objective that is to be achieved. There are several properties that are desired for these attributes, driven by the underlying utility theory foundation, as described below:

1. Complete: All *significant* attributes necessary to meet the decision objective are captured.
2. Practical: The necessary information can be obtained for all attributes.
3. Decomposable: Difficult to use attributes can be broken down into more understandable components.
4. Non-redundant: Avoid double counting; the attributes should be as independent from one another as possible.
5. Minimal: Selected attributes provide the decision maker with sufficient information, yet not are not so numerous that it is cost- or time-prohibitive to implement collection.

Meeting the desired properties for the decision attributes leads to transparent, defensible, and repeatable results. The Value-Focused Thinking methodology creates a strong basis for each alternative considered and is generalized so that it may be applied to alternatives with similar sets of attributes.

A key component of the methodological technique used is the means of aggregating disparate groups of attributes. When considering the aggregation methodology, a simple approach is to sum the attribute values that have been converted to a common dimension. In the absence of specific data to the contrary, this may be a suitable choice. The assumption with this approach is that all attributes are of equal importance to achieving the objective, which oftentimes is not the case. To account for the potential difference in relative importance, attribute importance values are assessed based on cybersecurity experts' opinions during an elicitation process. The elicitation of relative value addresses the needs to combine attributes with differing scales (e.g., height and weight) as well as capturing the relative importance of each attribute to achievement of the ultimate objective.

The elicitation of relative values was performed using four groups of experts representing different organizational types: Industry; DHS Cyber Security Advisors (CSAs); State, Local, Tribal, and Territorial (SLTT) Administration; and National Laboratories. The relative importance values for each attribute from each participant were collected and then averaged. Weights were determined for each attribute that reflected the relative importance of that attribute toward meeting the overall objective.

The evaluation methodology used to create the CPRI is defined below:

1. Identify program attributes relevant to the objectives of achieving cyber protection and resilience.
2. Using subject matter experts (SMEs), determine relative values of each attribute in achieving the overall objective.
3. Construct weights for each attribute using the elicited relative values.
4. For each alternative under consideration or program studied, apply the attribute weights to the corresponding selected attributes values.
5. Aggregate into a composite index value.

The CPRI is an indicator of likely effectiveness of cyber security and resilience programs and can be compared across a set of like cyber services and similar facilities. The composite score for each alternative or program studied provides guidance to a decision maker on the relative effectiveness of each alternative for achieving the intended objective. The composite index serves as a guide for the decision maker, who must often take other factors into account that could not be captured with the index. The average value across facilities can be regarded as setting a benchmark.

4.1 Identifying Program Attributes

The process of identifying attributes normally relies on determining pertinent stakeholders who will be making and/or be affected by the decision. Stakeholders include those who are close to the program under evaluation (i.e., decision makers, IT administrators, managers, and operators), as well as stakeholders who are not directly influenced by the program but have an interest in the evaluation (i.e., sponsors, regulatory authority, standards authority, or academia). The proper grouping of stakeholders is driven by the level of the decision maker and the decisions to be informed. For example, if the decision to be made is to determine the best portfolio of projects for a small component of a large agency, whose impact would be limited to the component, the stakeholders would consist only of members of that component. Alternatively, if the decision resides at the agency level, high-level members of that agency, as well as ranking members of other agencies that might be impacted, would be a more appropriate group of stakeholders to form the attributes.

The attributes for the CPRI include those of a cybersecurity program (i.e., management, personnel, controls, cyber dependencies, and incident response). If a stakeholder group begins with developing a comprehensive catalog of controls that are desirable in a cyber protection and resilience program, this creates a starting point for a list of attributes.

The CPRI is an aggregation of five main attributes, collectively known as CPRI Level 1 components (Figure 3).

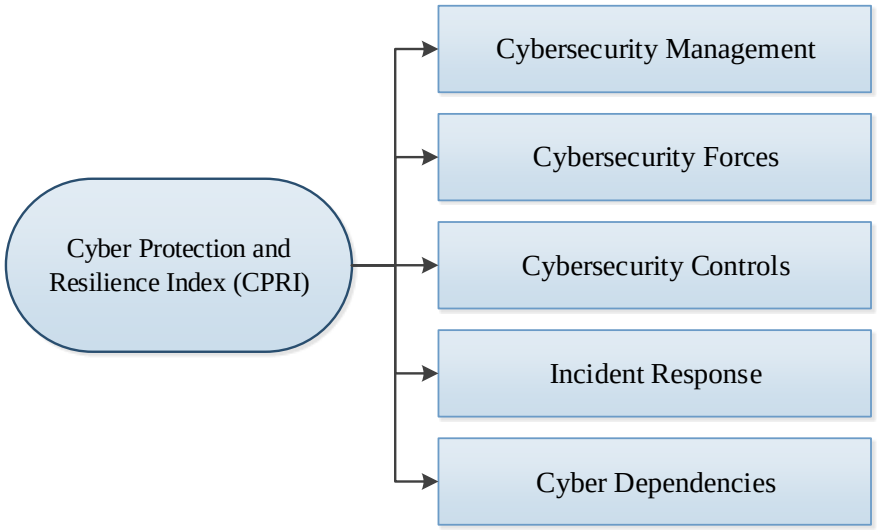


Figure 3. Cyber Protection and Resilience Index – Level 1 Components

Argonne performed the steps of creating the list of attributes and their classification into categories, in parallel with the NIST Cybersecurity Framework that was published in February of 2014 (NIST, 2014). Table 1 shows the correspondence between the top-level NIST category (Function) and the CPRI Level 1.

Table 1. Comparison between CPRI Level 1 and NIST Functions

CPRI Level 1	NIST Function	Definition
Cybersecurity Management	Identify	Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
Cybersecurity Forces Cyber Dependencies	Protect	Develop and implement the appropriate safeguards to ensure delivery of CI services.
Cybersecurity Controls	Detect	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
Incident Response	Respond	Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.
Incident Response	Recover	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired as a result of a cybersecurity event.

The NIST and CPRI frameworks are comprehensive in that all cybersecurity activities can be classified into either framework. As shown in Table 1, close parallels exist between CPRI and NIST's major categories, although the terminology of each differs slightly.

In the CPRI, each of the five Level 1 attributes is expanded into a multi-level hierarchy to capture the individual features of cyber protection and resilience programs.

Cybersecurity Management refers to an organization's plans and procedures for addressing cybersecurity issues. The CPRI divides this category into eight Level 2 subcomponents (Figure 4).

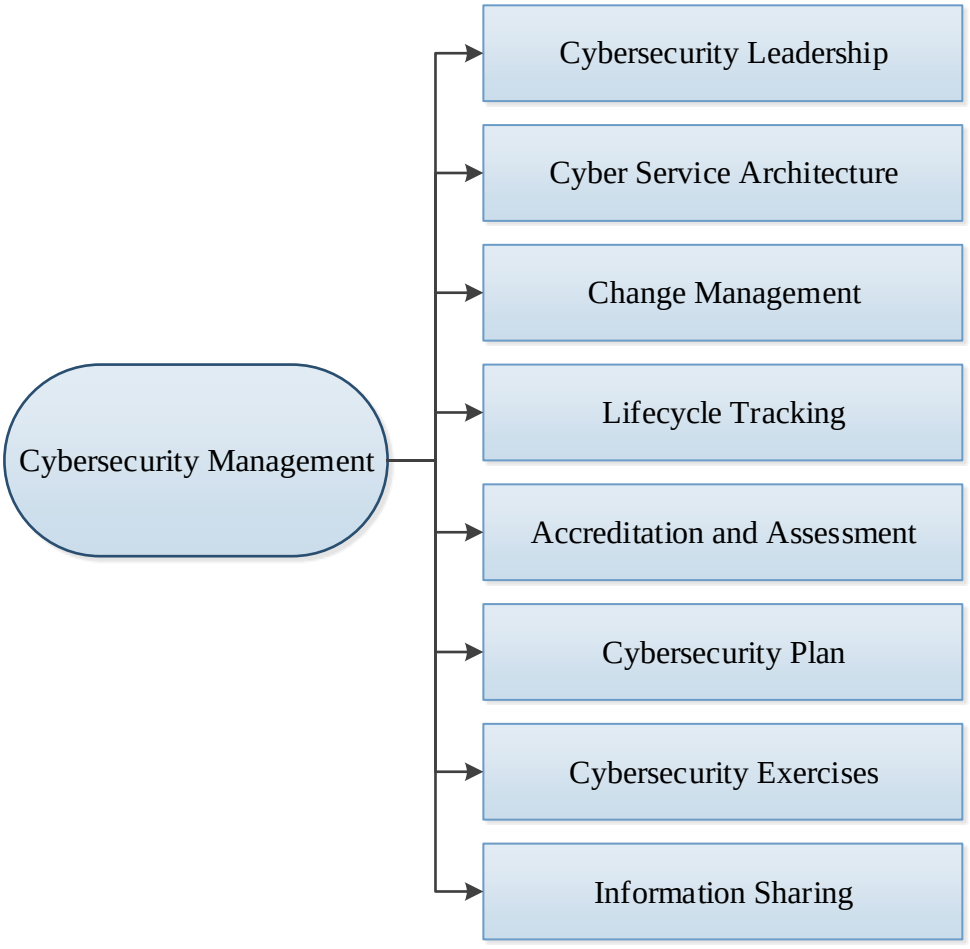


Figure 4. Cybersecurity Management – Level 2 Subcomponents

Table 2 describes the elements of the eight CPRI Level 2 Cybersecurity Management subcomponents.

Table 2. CPRI Level 2 – Cybersecurity Management Subcomponents Description

Cybersecurity Management Level 2	Description
Cybersecurity Leadership	Third-party contract arrangements that are designated to cybersecurity management.
Cyber Service Architecture	Documented cyber assets, networks, applications, inventory, and system architecture.
Change Management	Control procedures that are required for modifying the baseline configuration (e.g., policies, procedures, plans, inventory, and architecture) of the cyber system.
Lifecycle Tracking	Requirements, standards, and their enforcement.
Accreditation and Assessment	Formal external cybersecurity guidance and standards for identifying and implementing cybersecurity controls.
Cybersecurity Plan	Documented plans, procedures, and rules of behavior for individuals who access the information services.
Cybersecurity Exercises	Exercises for purposes other than compliance regularity as well as results documentation and approval.
Information Sharing	Reporting of cybersecurity incidents to outside organizations and communication with internal personnel.

Cybersecurity Forces refer to a special group of employees or contractors with protection and security duties. The CPRI divides this category into two Level 2 subcomponents (Figure 5).

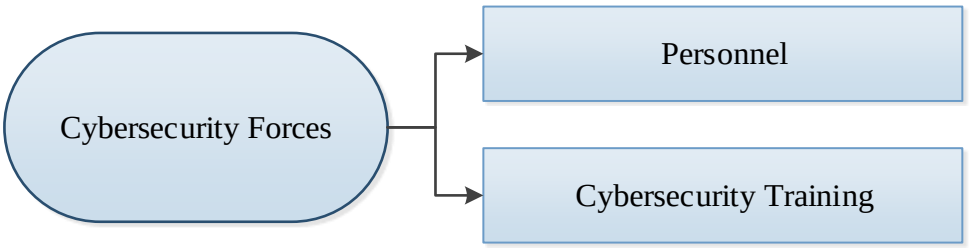


Figure 5. Cybersecurity Forces – Level 2 Subcomponents

Table 3 describes the elements considered for each of the two CPRI Level 2 Cybersecurity Forces subcomponents.

Table 3. CPRI Level 2 – Cybersecurity Forces Subcomponents Description

Cybersecurity Forces Level 2	Description
Personnel	Formalized positions that have accountable duties and specific policies, such as recurring background checks.
Cybersecurity Training	Schedule and updates.

Cybersecurity Controls refer to measures and processes for the detection of and response to cyber incidents (e.g., Unauthorized Access, Denial of Service [DoS], Malicious Code, and Improper Usage and Scans/Probes/Attempted Access). The CPRI divides this category into six Level 2 subcomponents (Figure 6).

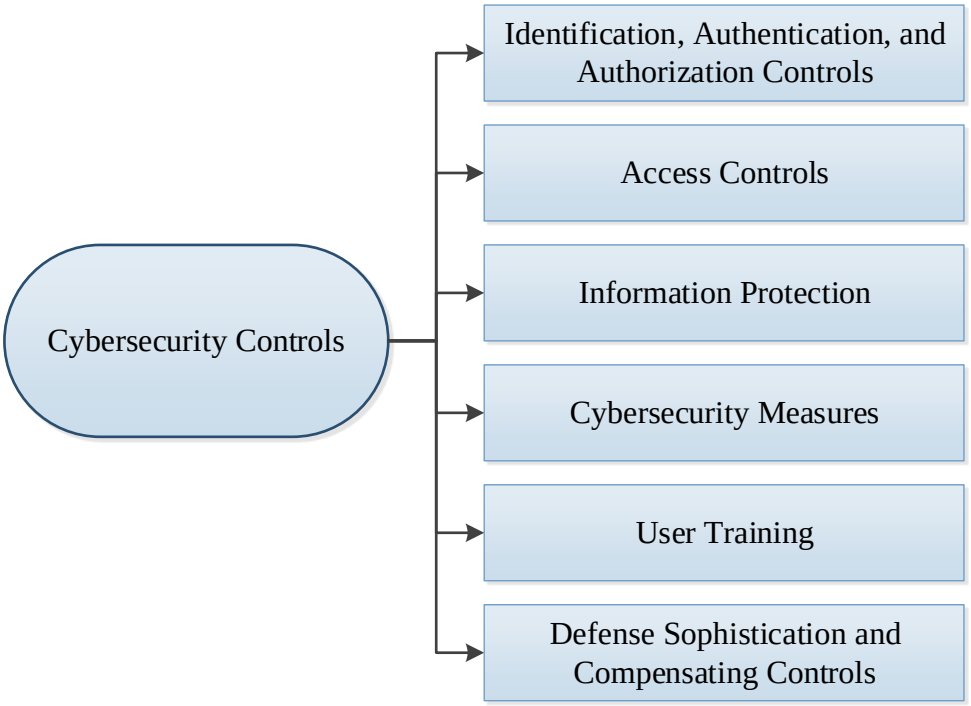


Figure 6. Cybersecurity Controls – Level 2 Subcomponents

Table 4 describes the elements considered for each of the six CPRI Level 2 Cybersecurity Controls subcomponents.

Table 4. CPRI Level 2 – Cybersecurity Controls Subcomponents Description

Cybersecurity Controls Level 2	Description
Identification, Authentication, and Authorization Controls	Privilege, administrative controls, credentials, password management, authentication controls, and the removal/modification of user permissions.
Access Controls	Business requirements for access paths to/from critical cyber services, remote access, and unauthorized access.
Information Protection	Identification and proper management of sensitive information.
Cybersecurity Measures	Procedures for detecting and managing malicious code, improper usage of equipment, and event logging.
User Training	Training schedule and review as well as network access for personnel.
Defense Sophistication and Compensating Controls	Procedures and architecture for increasing defense and controls (e.g., additional layers, moving target defense, and diverse platforms).

Incident Response refers to immediate and ongoing activities, tasks, programs, and systems that are in place to respond, recover, and adapt to the adverse effects of a cyber-event. The CPRI divides this category into two Level 2 subcomponents (Figure 7).

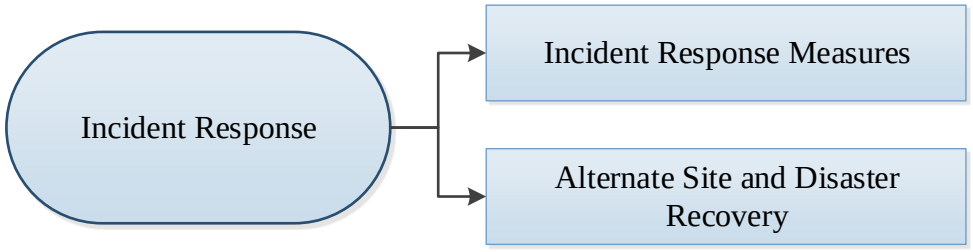


Figure 7. Incident Response – Level 2 Subcomponents

Table 5 describes the elements considered for each of the two CPRI Level-2 Incident Response subcomponents.

Table 5. CPRI Level 2 – Incident Response Subcomponents Description

Incident Response Level 2	Description
Incident Response Measures	Implementation, testing, review, and practice of documented incident-response plans and procedures.
Alternate Site and Disaster Recovery	Access to and testing of an alternative location as well as the existence of contingency and business plans.

Cyber Dependencies refer to the transfer and processing of data. The CPRI divides this category into four Level 2 subcomponents (Figure 8).

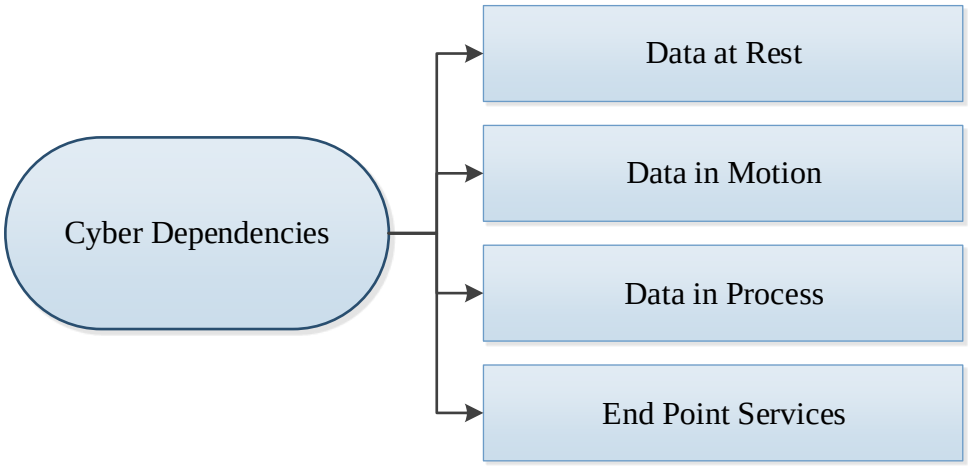


Figure 8. Cyber Dependencies – Level 2 Subcomponents

Table 6 describes the elements considered for each of the four CPRI Level-2 Cyber Dependencies subcomponents.

Table 6. CPRI Level 2 – Cyber Dependencies Subcomponents Description

Cyber Dependencies Level 2	Description
Data at Rest	Storage capabilities.
Data in Motion	Processes and equipment (e.g., switches, networks, and firewalls) that are used for the transfer of data.
Data in Process	Mainframes and clusters.
End Point Services	Hardware (e.g., desktops, laptops).

The next level in this hierarchy is the individual-attribute level. These are the specific program features whose selection corresponds to whether or not they exist within a specific program. For example, under the End Point Services Level 2 component, information is collected on the existence of end point hardware (e.g., desktops, laptops), impacts to the system if the endpoint services were not available, and the existence of plans to mitigate against the loss of these services.

Using the results of the elicitation process, a relative weight is calculated for each level of information and program feature that contributes to the overall CPRI. The CPRI is then calculated by aggregating its five Level 1 component values. For each component, an index corresponding to the weighted sum of its components is calculated. The overall CPRI therefore consists of a weighted sum of five Level 1 components (cybersecurity management, cybersecurity forces, cybersecurity controls, incident responses, and cyber dependencies), as shown in Equation 2. CPRI Weighted Linear Aggregation

.

$$CPRI = \sum_{i=1}^{5} w_i \, x_i$$

Equation 2. CPRI Weighted Linear Aggregation

where: *CPRI* is the relative Cyber Protection Resilience Index (ranging from 0 to 100);

w_i is the scaling constant, (weight; a number between 0 and 1) indicating the relative importance of component i (i = 1, 2, 3, 4) in increasing resilience and protection; and

x_i is the index value of component i of cyber protection and resilience (i.e., cybersecurity management, cybersecurity forces, cybersecurity controls, incident responses, and cyber dependencies)

This process results in an overall CPRI, ranging from 0 (low protection and resilience) to 100 (high protection and resilience) for the CCS analyzed, as well as an index value for each Level 1 through Level 3 component. This method to characterize the protection and resilience of a critical cyber system makes it possible to consider the cyber systems across all CI subsectors and to compare the different protection and resilience enhancement options for the studied system.

4.2 Determining Weights for Attributes

Four groups of SMEs, each from a different type of organization, participated in the elicitation process:

- Industry,
- DHS CSAs,
- SLTT Governements, and
- National Laboratories.

During each elicitation, the SMEs assigned a relative importance value for each level of the CPRI hierarchy and each individual feature contributing to the resilience and protection of CCSs.

The relative importance of each CPRI attribute was first defined in general for all threats. Separate elicitations were conducted for specific threats and hazards:[1]

- Distributed Denial of Service (DDoS);
- Natural Disaster;
- Remote Malware (Confidentiality); and
- Destructive Malware (Integrity).

Since time and effort limitations made it impractical to elicit separate sets of importance values for each attribute for each threat type, a slightly simplified approach was taken. In this approach, a threat-specific weight is obtained for each first subcategory (Level 2) and then also a weight for the main category (Level 1). For example (Figure 5), the CPRI Level 1 Cybersecurity Forces has two Level 2 categories, Personnel and Cybersecurity Training. Relative importance values were first elicited for Personnel and Cybersecurity (Level 2) and then between each Level 1 component. The variation in attribute weights associated with specific threats is incorporated when these Level 2 weights are included in the product of the Level 3 weights.

As previously mentioned, the value of the CPRI varies from 0 to 100. The value of the CPRI is 0 if the organization does not have any of the elements that contribute to the index, and 100 if the organization has implemented the best options for all the elements contributing to the CPRI. The CPRI is therefore an indicator of the degree to which the important elements contributing to cybersecurity have been implemented by a given organization.

Interpretation and implication of the index are important for decision makers to understand. A value of 0 does not mean that the facility has no protection or resilient features or that every type of threat will lead to its immediate shutdown. The zero value only indicates that the organization does not have any of the attributes that were collected for the CPRI. Some external elements that could be indicative of the protection and resilience of the CCS are not captured in the CPRI calculation, such as the capabilities of the emergency services sector that will affect the ultimate consequences to the organization. Similarly, a CPRI of 100 does not mean that the organization is perfectly protected from and resilient to types of events. The CPRI score is an indication of the relative protection and resilience of existing CCS attributes with respect to the highest and lowest levels of the index. However, a value of 50 does not mean that 50% of the elements considered in the CPRI calculation are in place within the organization. A CPRI of 50 can be obtained in many different ways by combining different components of protection and resilience. If the value of the CPRI increases, the cybersecurity capabilities of the organization are improved.

4.3 Data Collection

A question set was developed to help identify the gaps in the cybersecurity of CI and to characterize the existing cyber protection and resilience programs. This question set, called the Cyber Infrastructure Survey Tool (C-IST), is organized to capture the required information for calculating the CPRI, and its structure is based on the CPRI hierarchy. The C-IST contains approximately 78 parent questions with a fixed set of possible response options (a forced-choice

[1] The DHS Office of Cybersecurity and Communications provided the list of required threat scenarios.

format) to improve the objectivity and repeatability of the assessment and to measure the attributes detailed previously.

This assessment is intended to benefit Federal, SLTT, and private stakeholders by identifying and analyzing the cyber protection and resilience measure practices of CI providers. It supports the analysis of cybersecurity planning and resource allocation.

The C-IST assessment consists of a 2-hour interview by a DHS CSA with an organization's key cybersecurity personnel. The CSA engages in conversation about the CCS with these personnel to ensure that all pertinent information is recorded.

Three main elements allow users to ensure the uniformity and reproducibility of the data collected—"helps" and explanations, training; and quality assurance (QA) review.

The C-IST "Helps" explain the definition for each question and what information it is intended to capture. CSAs are trained not only in how to conduct the visits, including the interviews with the CI owners and operators, but also in the intent of the different questions and in how they are used to calculate the CPRI. The collected data are then verified through a QA review process.

The training, "Helps" and QA processes are an integral part of the larger methodology as they maintain the reproducibility of the collected information and the disseminated products. In addition, verifying the data before producing the CPRI reduces the overall time it takes to return a final product to the owner or operator. Beyond its benefits for the product, the QA process also has several other benefits. The CSA reviews serve as continual training opportunities that reinforce, over time, a consistent application of the methodology. The process can also highlight problems that may exist in the question set, such as unclear questions or incomplete sets of answers. The questions and their potential responses can then be re-evaluated following the identification of a pattern of errors. Often, questions or "Helps" are revised to enhance their clarity and consistency of interpretation.

The C-IST provides public- and private-sector organizations with an effective, repeatable data-collection technique for cybersecurity operations. In addition to the overall index, the collected information allows the calculation of component indices for key categories of protection and resilience programs. The calculation tool presents the overall index as well as the component index values (i.e., Level 1, 2, and 3) in the form of an interactive dashboard.

4.4 Visualization Tool

The dashboard is an interactive visualization tool that can be used to perform sensitivity analyses on hypothetical program modifications (Figure 9).

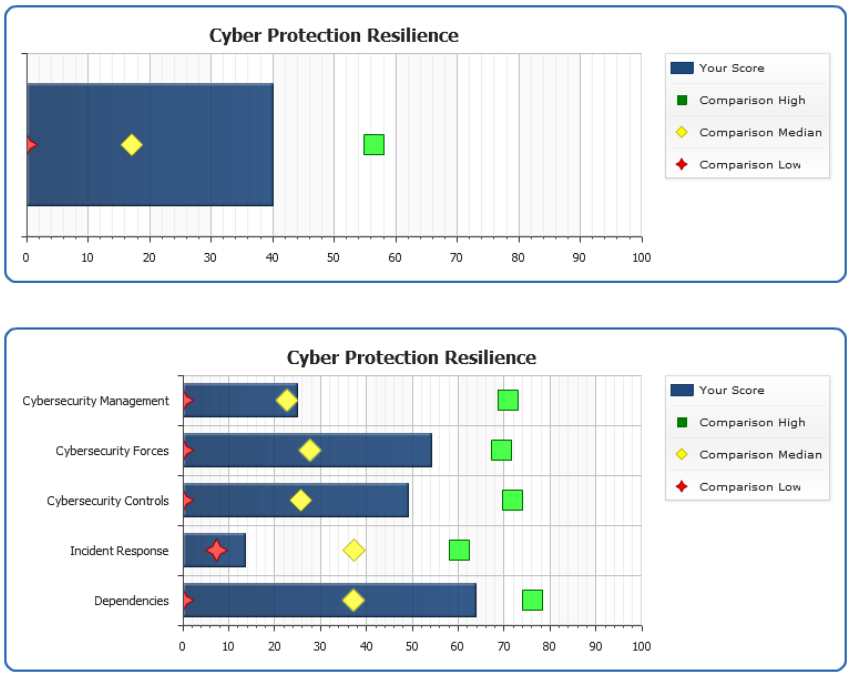


Figure 9: Illustrative Screenshot of the CPRI Dashboard

The CPRI dashboard identifies the respondent's current cyber protection and resilience score along with the high, low, and median cyber protection and resilience scores of other respondents with similar CCSs. Upon completion of the assessment, respondents can assess themselves and compare their practices to similar organizations. Existing values are presented as a blue rectangle; the comparison values with other organizations in the same comparison group that have achieved low, median, and high index values, are represented as a red star, yellow diamond, and green square, respectively.

The Dashboard is an interactive tool in that users can change the characteristics of the components contributing to the CPRI and then compare a scenario value to the existing value, assessed during the visit, to see if cyber resilience and protection have improved. The dashboard allows the user to see—in real time—the impacts of component modifications on the overall CPRI value as well as on the specifically selected and modified components. For example, an organization may want to know its relative increase in protection and resilience if it added cybersecurity training for the cybersecurity force to its current practices. With the scenario function, the organization can utilize the tool to calculate a new CPRI. Figure 10 shows how this result is obtained; existing characteristics are shown in dark blue, and the scenario values are shown in light blue.

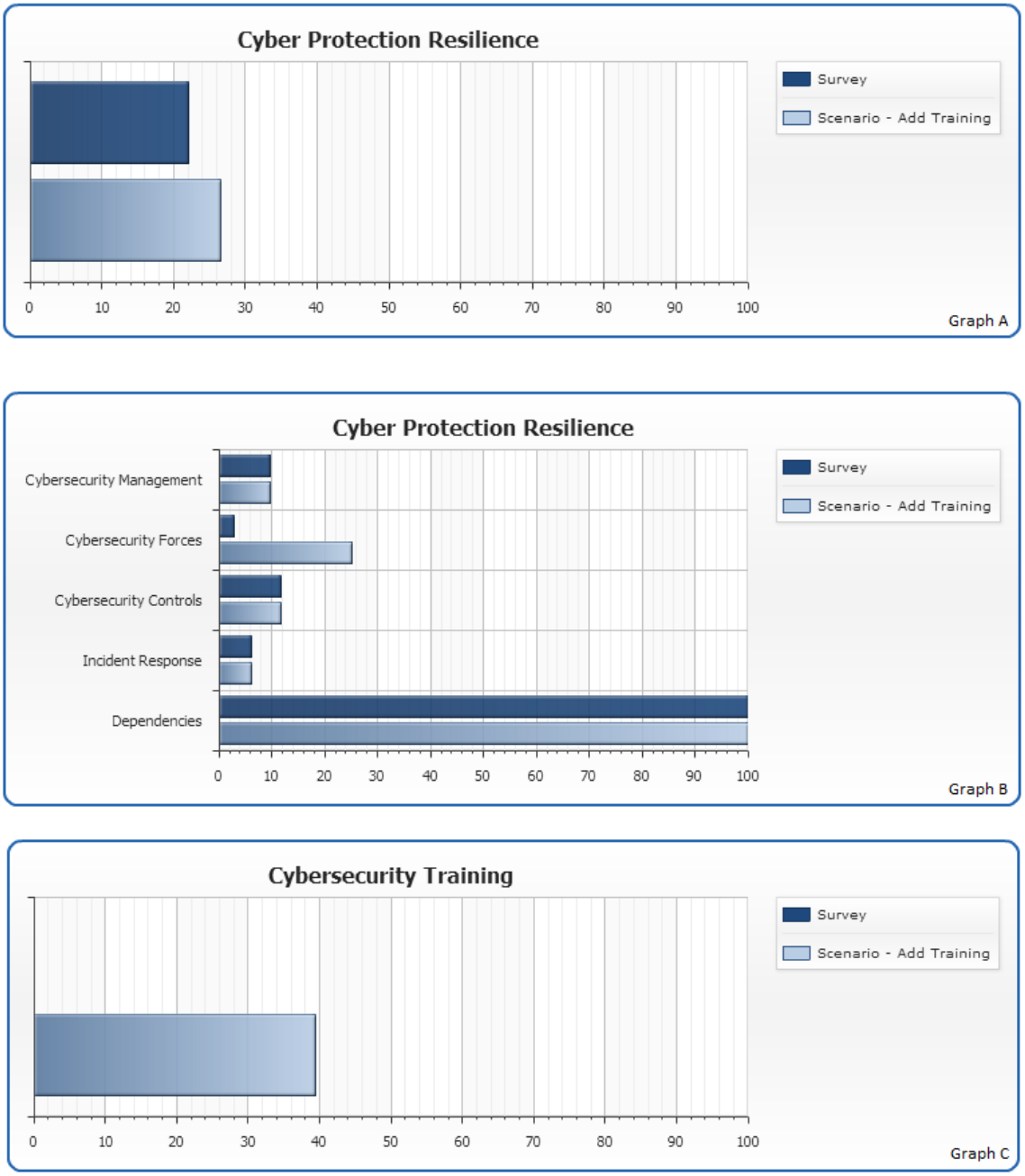


Figure 10: CPRI Training Scenario

When the C-IST was initially completed by the CSA, the organization indicated it does not have training processes in place. Therefore, as shown in Graph C of Figure 10, it received a score of 0 for the Cybersecurity Training component (there is no dark blue rectangle). The tested scenario was the addition of in-house/in-formal training, utilizing annual classroom, on-the-job, and web-based training on risk management; the new score of this CPRI component is now 39. Cybersecurity training is a component of Cybersecurity Forces, so Graph B of Figure 10 shows the impact of adding cybersecurity training on the Cybersecurity Forces score. The value of the Cybersecurity Forces score increases from 3 to 25; all other Level 1 components remain the

same. Finally, the overall CPRI also increased to reach a score of around 26, as shown in Graph A of Figure 10.

The CPRI Dashboard displays the index value for a general threat or hazard; however, a threat "overlay" allows the user to select a specific threat (e.g., DDoS; Natural Disaster; Remote Malware [confidentiality]; and Destructive Malware [Integrity]) and recalculate the CPRI.

Figure 10 shows the overall CPRI value along with the high, median, and low values recorded to date. Currently, the high, median, and low values are those from the entire population of surveyed organizations. As the number of completed surveys expands, it will display these values based only on surveys of similar organizations with similar critical services within a specific sector. This increase in survey data will thus improve the relevance of the results as an indicator of relative program effectiveness. The comparison across a set of similar organizations serves as an aid to support decision-making.

The ability to change the parameters and immediately see the impact, combined with the threat scenarios, makes the CPRI Dashboard a useful tool for managing cyber protection and resilience-related decisions about CI facilities.

5 Methodology Advantages and Limitations

The decision-analysis methodology that was used in the development of the C-IST and the CPRI specifically integrates the necessary elements for assessing the cyber protection and resilience of a CCS. The methodology integrates not only cybersecurity management and cybersecurity controls that are traditionally part of cybersecurity-analysis methodologies but also operational elements, such as cybersecurity forces, incident response, and cyber dependencies. The default weighted values of the index are based on a general threat that, through consistent application, allows for an index that is suitable for many organizations. However, the CPRI can also be defined for four specific threats: DDoS, Natural Disaster, Remote Malware, and Destructive Malware.

The methodology ensures reproducible results through the organization of the cyber protection and resilience components into different levels of information and by ranking the relative importance of these components in terms of cybersecurity management, cybersecurity forces, cybersecurity controls, incident response, cyber dependencies, and ultimately protection and resilience. Furthermore, by defining a consistent index for cyber protection and resilience measures, owners and operators can compare different assets in the same sector, and oversight or coordinating bodies can formulate regional and sector cyber protection and resilience policies or practices. These comparisons also highlight differences in the way various sectors approach cybersecurity.

The CPRI allows not only for a comparison between CCSs but also for a characterization of the most effective measures for improving cyber protection and resilience. The CPRI Dashboard lends additional significance to the CPRI metric and what it means for an organization's overall cybersecurity posture. The CPRI Dashboard allows users to take the information that emerges from calculating the CPRI and to use it for daily operations, informing investment decisions, and strategic planning.

The flexibility of the methodology allows it to be used in different assessment programs. It allows for reproducible results, comparison of an organization's cybersecurity derived from consistent methods, and a flexible approach that can be altered to fit the individual needs of sectors, subsectors, or systems.

It is important to note that the CPRI is a relative measure. A high CPRI does not mean that a specific event will have minimal consequences. Simply stated, the CPRI allows comparison of different levels of cybersecurity (protection and resilience) for CI. The scaling of the index[2] is such that improvement from 20 to 40 is equivalent to improvement from 60 to 80. Determining an organization's CPRI and how different options affect it can be used to identify the most effective ways to improve an organization's overall cybersecurity.

Although the CPRI has many advantages, it also presents some limitations. The main limitations of this tool relate to the interpretation or use of the collection tool and associated index. First, regarding the interpretation of a defined CPRI value, it is important to remember that the CPRI is a relative indicator of CI cyber protection and resilience based on information that has been collected in a single session. Since data collection is a voluntary program, the time taken at the facility to answer all of the CPRI questions in detail is always a factor. In addition, since the

[2] As determined from elicitations of cybersecurity experts.

CPRI must be applicable across all types of organizations, the assessor's knowledge of specific technical and operational functions is also a factor.

Second, the CPRI characterizes the cyber protection and resilience for a specific system. CPRI values that are defined for different systems cannot directly be used to determine the cybersecurity in place for an entire region or CI sector. The CPRI of different cyber systems in a region give an indication of the cybersecurity of the region, but other elements characterizing the region (e.g., economy, environment, and institutional services) also affect regional cybersecurity.

The CPRI should be used as part of an overall risk management program. It provides important information about the protection and resilience of a given organization's critical cyber system and how that system compares to other similar systems. Other factors such as location, specific vulnerabilities, and a cost-benefit analysis should also be utilized to ensure a complete risk picture. Furthermore, the cyber assessment should also be combined with an assessment of physical protection and resilience measures.

6 Future Developments

Currently, the C-IST and CPRI are still in their early stages of use within the DHS cyber community. Upon maturity of these tools, a year-over-year comparison of CPRI scoring will be possible, allowing a company not only to benchmark against organizations within their sector but also to benchmark against the organization's own historical data. Furthermore, additional analysis will be conducted to highlight key focus areas and identify possible enhancements for both the C-IST and CPRI. In particular, additional elicitations will be held to ensure that the CPRI and additional threat scenarios are representative of the current cybersecurity landscape. Since the technologies and practices of cyber protection and resilience are constantly changing, periodic reviews will also identify any new attributes that are necessary.

This page intentionally left blank.

7 Conclusion

The CPRI is an indicator of the effectiveness of an organization's cyber protection and resilience program. Argonne National Laboratory created a methodology to calculate and utilize the CPRI, by working with stakeholders in identifying, classifying, and weighing the relative importance of attributes that contribute to an organization's cyber protection and resilience program.

Through the elicitation process and the use of multi-attribute decision analytics, Argonne has been able to provide an index that can be utilized within all 16 CI sectors defined by DHS. The CPRI can be utilized by the surveyed organization for benchmarking purposes against itself as time progresses. In addition, the current structure of the CPRI allows for simplified modification of attributes without needing to work through the entire elicitation process. The CPRI is flexible in that it can be applied not only for a general threat scenario but also for four specific threats (DDoS, Natural Disaster, Remote Malware, and Destructive Malware). As such, the CPRI for the C-IST has accomplished the goal of fulfilling all four challenges for effectively measuring an organization's cyber protection and resilience program: (1) combining diverse attributes, (2) applying to specific organizations, (3) including subjective assessments, and (4) evaluating potential program changes.

This page intentionally left blank.

8 References

CFATS (Chemical Facility and Anti-Terrorism Standards) (2009). *Risk-Based Performance Standard (RBPS) 8: Chemical Facilities Anti-Terrorism Standard*, Risk-Based Performance Standards Guidance 8 – Cyber, 6 CFR Part 27, available at http://www.dhs.gov/xlibrary/assets/chemsec_cfats_riskbased_performance_standards.pdf, accessed July 7, 2017.

DoD (U.S. Department of Defense) (2003). *Instruction 8500.2 Information Assurance Implementation*, available at http://www.cac.mil/docs/DoDD-8500.2.pdf, accessed July 7, 2017.

DHS (U.S. Department of Homeland Security) (2009). *Catalog of Control Systems Security: Recommendations for Standards Developers*, Control Systems Security Program, National Cyber Security Division, available at https://www.smartgrid.gov/files/DHS_National_Cyber_Security_Division_Catalog_Control_Systems.pdf, accessed July 7, 2017.

DHS (2015a). *Critical Infrastructure Sectors*, available at http://www.dhs.gov/critical-infrastructure-sectors, accessed July 7, 2017.

DHS (2015b). *ICS-CERT*, Assessments, available at http://ics-cert.us-cert.gov/Assessments, accessed July 7, 2017.

ISO/IEC (International Organization for Standardization/International Electrotechnical Commission) (2009). *ISO/IEC 15408:2009, Information Technology — Security Techniques — Evaluation Criteria for IT Security*.

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

Keeney, R., and H. Raiffa, (1976). *Decision Analysis with Multiple Objectives*, Wiley and Sons, Inc., New York.

NERC (North American Electric Reliability Corporation) (2006). *NERC 1200 and CIP-002 through CIP-009 Comparison*, Version 3, available at http://www.netsectech.com/wp-content/uploads/2013/05/WP_NERC_CIP_Analysis_NST.pdf, accessed July 7, 2017.

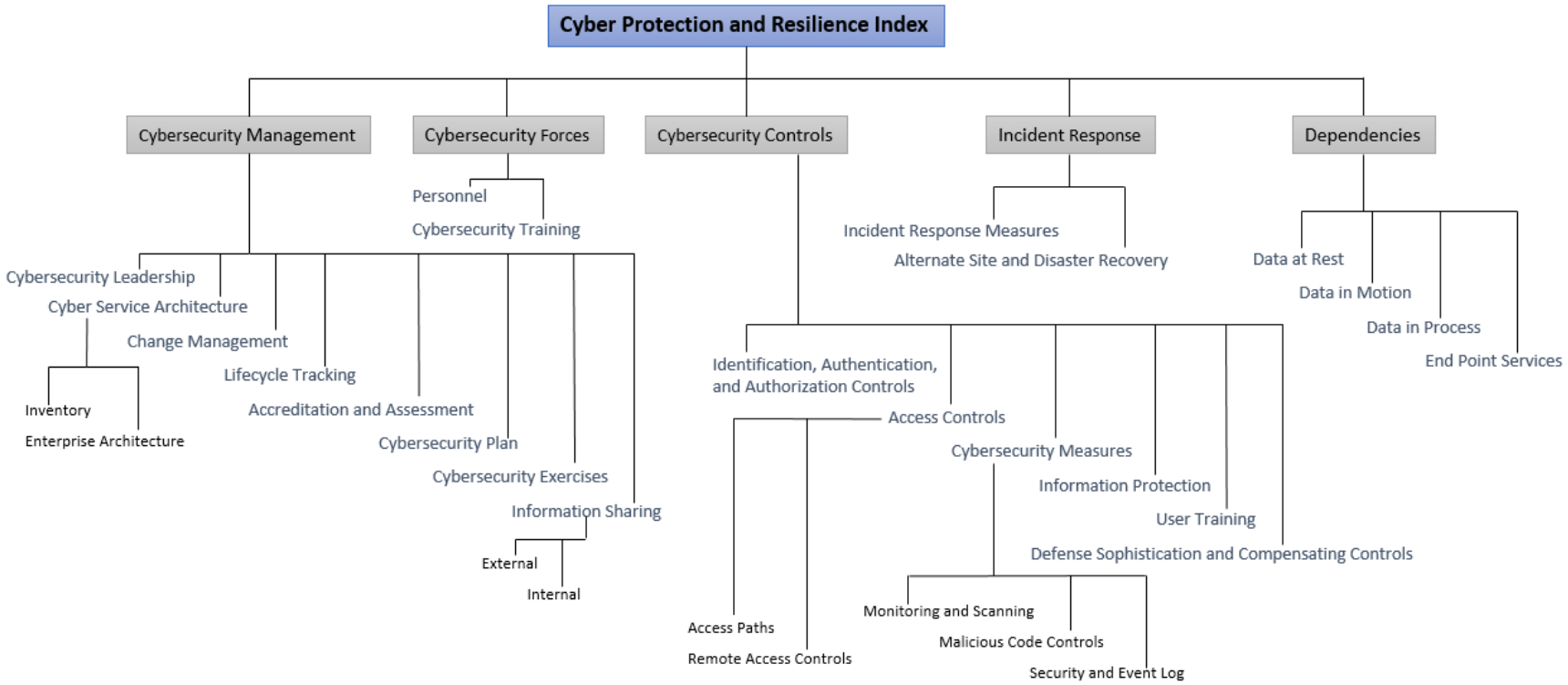
NIST (National Institute of Standards and Technology) (2005). *Recommended Security Controls for Federal Information Systems*, Rev. 3 with Appendix I, ICS Controls, NIST Special Publication 800-53, available at http://infohost.nmt.edu/~sfs/Regs/sp800-53.pdf, accessed July 7, 2017.

NIST (2011). *Guide to Industrial Control Systems Security*, NIST Special Publication 800-82, available at http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf, accessed July 7, 2017.

NIST (2014). *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.0, available at http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214-final.pdf, accessed July 7, 2017.

U.S. President (2013). “Improving Critical Infrastructure Cybersecurity,” Executive Order 13636, *Federal Register*, 78 (33):11739–11744, Feb. 19, 2013, available at http://fas.org/irp/offdocs/eo/eo-13636.pdf, accessed July 7, 2017.

Appendix: CPRI Level Breakdown



This page intentionally left blank.

Global Security Sciences Division
9700 South Cass Avenue, Bldg. 203
Argonne, IL 60439-4854

www.anl.gov