MP120053, Rev. 1

Cyber Resiliency Metrics, Version 1.0, Rev. 1

Deb Bodeau, Rich Graubart, Len LaPadula, Peter Kertzner, Arnie Rosenthal, Jay Brennan

April 2012

Dept. No.: G020
Project No.: 05MSR160-JT

Bedford, MA

This page intentionally left blank.

Abstract

This white paper describes the initial representative set of cyber resiliency metrics identified by the Assessment task of the Resilient Architectures for Mission Assurance and Business Objectives (RAMBO) project under the FY11 MITRE Innovation Program. This set of metrics is expected to evolve in response to practical experience as well as to the ongoing refinement of the cyber resiliency engineering framework.

This page intentionally left blank.

Table of Contents

This page intentionally left blank.

1 Introduction

The need for cyber resiliency – for missions and business functions to anticipate, withstand, recover from, and evolve in the face of persistent, stealthy, and sophisticated attacks focused on the cyber resources on which they depend – is increasingly recognized. Engineering and operational decisions to improve cyber resiliency need to be supported by suitable metrics and assessment processes. In addition to supporting decisions, metrics serve to improve understanding. This white paper describes metrics work done under the Resilient Architectures for Mission Assurance and Business Objectives (RAMBO) Assessment task in FY11, including

- Establishing an approach to identifying, characterizing, and defining cyber resiliency metrics;
- Identifying an initial representative[1] set of technical and cost metrics for cyber resiliency; and
- Prototyping a tool that enables users to identify cyber resiliency metrics from the representative set which could be relevant to their needs.

2 Metrics Approach

The approach taken to identifying cyber resiliency metrics has been to cast a broad net, constructing a representative set of metrics that includes

- Metrics for different uses – in particular, metrics that support operational decisions and metrics that support engineering decisions[2];
- Metrics applicable to different architectural layers or classes of resources, e.g., systems, systems-of-systems, applications, knowledge bases or data stores, communications, and specific technologies;
- Metrics that reflect different characteristics, including timeliness, capability, and confidence;
- Metrics in different forms – quantitative, semi-quantitative, and qualitative;
- Metrics repurposed from – or that reuse and repurpose data used for – metrics in other engineering disciplines, most notably security metrics; and
- Metrics specific to the technologies being investigated under the RAMBO project.

The representative set of metrics thus includes metrics with varying degrees of rigor, and which address very different parts of the cyber resiliency problem space. The set is representative, with no claims of completeness; it is intended to serve as a starting point for identification and tailoring of metrics to be used in a specific situation. The set is unstructured; metrics are listed rather than organized into subsets. This broad-net approach contrasts with a minimalist approach that strives to define a few metrics, applicable to a narrow but well defined and well modeled part of the problem space, with a high degree of rigor.

[1] The set is representative in that it addresses the full range of cyber resiliency objectives and approaches, as well as architectural layers and dimensions of cost, identified in the Cyber Resiliency Engineering Framework (Bodeau and Graubart 2011).

[2] Resilience metrics can also support organizational decisions, in particular decisions to make changes to governance structures and processes. To avoid duplicating effort, organizational resilience metrics as described in (Allen, et al., 2010) were deemed outside the scope of Version 1.0 of the cyber resiliency metrics.

The rationale for this broad-net approach is presented below.

2.1 Multiple Stakeholders Seek Metrics

A wide variety of stakeholders need to make decisions which could be informed by cyber resiliency metrics. These include

- Mission commanders (or business function heads). Cyber resiliency metrics can be used as inputs to operational metrics (e.g., Measures of Effectiveness), which help mission commanders understand how well they can perform their missions (or business functions) and whether they need to consider alternative courses of action based on degradation of cyber resources.
- Cyber defenders (e.g., CND staff[3]; staff in a Resiliency Operations Center, a Cyber Operations Center, or a Cyber Security Operations Center). Cyber resiliency metrics can help defenders understand the current posture of cyber resources, as well as trends with respect to adversary activity. Cyber resiliency metrics can also help defenders select cyber courses of action and monitor the effectiveness of course-of-action execution.
- Officials responsible for mission continuity, business continuity, or contingency planning. Such officials need to factor cyber resiliency concerns into planning. Cyber resiliency metrics can help them identify targets and thresholds.
- Senior IT/ICT providers (e.g., the manager of a data center that provides resources to multiple missions or users, the provider of a common infrastructure such as a network or of a set of shared services such as identity management). Such providers can use cyber resiliency metrics as part of defining or characterizing their offerings.
- Senior information security or information assurance (IA) staff (e.g., Chief Information Security Officer). Cyber resiliency objectives overlap with security objectives (see (Bodeau and Graubart 2011) for further discussion). Cyber resiliency metrics enable security staff to determine how well cyber resiliency objectives (and the related security objectives) are being achieved.
- Program managers (as informed by systems engineers and architects). Cost and technical metrics for cyber resiliency can inform decisions related to cost-benefit trade-offs of cyber resiliency investments and decisions related to programmatic risk management.
- Architects and systems engineers. Cyber resiliency metrics can inform decisions about which cyber resiliency approaches to apply, where, how, and in what timeframe. Cyber resiliency metrics can also be used in cost-benefit analyses and risk analyses.
- Cyber Resiliency Researchers. Cyber resiliency metrics can inform decisions about whether and when a given implementation of a cyber resiliency approach is worth pursuing further.
- Product vendors and solutions providers. Cyber resiliency metrics can be used to position offerings favorably.

To address the concerns of diverse stakeholders, a representative set of cyber resiliency metrics is more useful than an attempt to cover completely a narrow subset of the problem space.

[3] Examples include a Tier 2 or 3 Computer Network Defense (CND) Service Provider or CNDSP; see (Chairman of the Joint Chiefs of Staff, 2011).

2.2 Metrics-Informed Decisions Can Apply to Different Scopes

As indicated by the list of different stakeholders, the scope of a cyber resiliency engineering or operational decision – the set of resources to which the decision applies – can range from a single product to a mission/business segment or a cross-organizational system-of-systems. A set of metrics that addresses a single scope cannot serve multiple stakeholders. The representative set therefore includes metrics for very different scopes, while noting that some metrics can be applied to multiple scopes. In particular, it includes metrics that could be applied across an enterprise as well as metrics specific to implementations of RAMBO technologies.

In addition, assessments of cyber resiliency must be performed in real-world environments, subject to organizational and operational constraints on what types of data can be gathered and what resources can be applied to analyzing that data. Thus, a metric that is both meaningful and easily evaluated in one environment can require extensive re-interpretation and a costly evaluation process in another environment.

2.3 Multiple Characteristics Need to Be Described by Metrics

Three broad types of metrics are relevant to cyber resiliency:

- Technical metrics, which evaluate the behavior of technologies and of technology-dependent mission/business processes (particularly cyber defense processes);
- Organizational metrics, which evaluate organizational processes for resilience (in which cyber resiliency is – or should be – a consideration)[4];
- Cost metrics, which evaluate the potential cost of (or organizational level of concern for) using a cyber resiliency approach, solution, or product, or for improving organizational processes. Note that cost is multi-dimensional, including not only the dollar costs of acquiring or integrating a solution, but also support costs and consequential costs (e.g., mission impacts, changes in programmatic risk).

The initial representative set of metrics includes both cost and technical metrics.

A technical metric (and in some cases, a cost metric) may be meaningful only in the context of a specific technology, type of technology, or architectural layer. The initial representative set of metrics includes metrics specific to a technology or architectural layer. It is possible to identify general metrics (e.g., level of capability, time between initial damage and given level of capability) which can be interpreted for (and thus tailored and applied to) different scopes. Follow-on work may in fact establish relationships among metrics, to improve the rigor and comprehensiveness of the representative set. However, a stakeholder who is interested in supporting a specific decision may have no interest in the relationships between the specific interpretations and the more general metric.

2.4 Ranges of Values Can Differ in Form

The set of possible values for a metric can be expressed in quantitative, qualitative, or semi-quantitative[5] terms. Each approach has both benefits and drawbacks.

[4] Organizational metrics can be developed following the CERT® Resilience Management Model (Allen, et al., 2010), and (with the exception of areas not addressed by the RMM) are beyond the scope of the RAMBO Assessment task.
[5] See (Risk Steering Committee, 2010) for more on the distinction between these types of values.

Quantitative value scales most easily support cost-benefit analysis and combinations of more-specific metrics to produce higher-level metrics. Quantitative values can use interval, ratio, or absolute scales (Brennan, et al., 2009), and offer precision and rigor. However, the meaning of the quantitative results may be unclear (Is this number good or bad? Is this difference in values meaningful or insignificant?), requiring a qualitative interpretation. Additionally, the rigor of quantification is significantly lessened when subjective determinations are "buried" within quantitative evaluation processes. Functional combinations are easier to compute automatically, but interfaces often have the misleading side effect of appearing to increase the number of significant digits. Finally, the benefits (in terms of rigor, repeatability, and reproducibility of assessment results) can be outweighed by the costs (in terms of expert time and effort, and possibly in the deployment and use of tools) and calendar time required to make sound evaluations of quantitative metrics.

Qualitative value scales[6] most strongly support communication. However, the range of values in a qualitative assessment scale is typically small (e.g., very low, low, medium, high, very high), making relative prioritization or comparison difficult. Additionally, unless each value is very clearly defined or is characterized by meaningful examples, different experts could produce significantly different assessments. The repeatability and reproducibility of qualitative assessments are increased by annotation of assessed values (e.g., "high because ….") and by using tables or other well-defined functions to combine qualitative values.

Semi-quantitative value scales can provide the benefits of both quantitative and qualitative assessment: Bins (e.g., 0-15, 16-35, 35-70, 71-85, 86-100) or representative numbers (e.g., 1-10) translate easily into qualitative terms that support communication (e.g., "a score of 95 is very high"); the role of expert judgment in assigning values is more evident than in a purely quantitative approach; and (if the scales or sets of bins provide enough granularity) relative prioritization among results is better supported than in a purely qualitative approach. A semi-quantitative assessment approach requires well-defined order-preserving functions to combine values, and the number of significant digits must not be allowed to appear to increase as values are combined. As with the non-numeric categories or levels used in a well-founded qualitative approach, each bin or range of values needs to be clearly defined and/or characterized by meaningful examples.

2.5 Use Metrics Selectively

Evaluating and tracking metrics requires resources. Thus,

- Existing metrics and measurement data should be repurposed as feasible. Fortunately, metrics already in use (or the data collected for in-use metrics) can be repurposed for cyber resiliency. Such metrics include cyber security metrics related to availability and integrity[7], as well as performance metrics.
- A few well-defined metrics should be selected for evaluation and/or tracking. A large number of metrics can be challenging to interpret as well as to evaluate and maintain. (Boyer, et al., 2008)

[6] Nominal scales, as defined in (Brennan, et al., 2009), are an example of qualitative assessment scales.

[7] However, cyber resiliency involves more than achieving the information security goal of availability and integrity. Cyber resiliency includes not only protecting critical resources from degradation or denial of service prior to or during an attack, but also assessing their integrity or quality, recovering or reconstructing mission functionality, and evolving to be better prepared for new threats.

- The utility of each metric that is evaluated or tracked should be validated. Does the metric provide meaningful information ? That is, can the information provided by the metric be used to support the decisions that can be made, given real-world constraints (as contrasted with, for example, decisions that could be made in a perfect world)? How relevant is the information provided by the metric to the decisions it supports? That is, does it directly answer a question of interest to decision-makers, or is it an indicator with a tenuous relationship to decision-makers' questions? As metrics are used, their utility should be revalidated periodically.

3 Initial Set of Cyber Resiliency Metrics: Templates and Metrics

The initial set of cyber resiliency metrics assembled in FY11 consists of metrics templates, a representative set of cyber resiliency metrics (cost as well as technical metrics), and completed templates for some cost and technical metrics. Systems engineers, architects, and cyber defenders can use the set presented in Appendix B to identify metrics that are potentially relevant to their situations. From these, they can select a few metrics which are most amenable to evaluation and tracking, use the metrics template to specify how those metrics will be evaluated and tracked in their environments, use the metrics (evaluating them, tracking them over time or comparing values in support of engineering decisions), and validating the utility of the metrics.

3.1 Templates

A small amount of information can be used to characterize a technical cyber resiliency metric:

- A brief definition (e.g., time between the decision to change filtering rules and when the new rules are fully effective; percentage of mission-essential applications for which at least two instantiations are available).
- The types of decisions it is intended to support (operations, engineering, or both).
- The cyber resiliency goals and objectives toward which it measures progress.
- The cyber resiliency approaches[8] for which it measures effectiveness.
- The architectural layers or sets of cyber resources to which it applies.
- How the metric is evaluated (e.g., by continuous monitoring and risk scoring (CMRS) tools, by analysis of log data, by Red Team observation and analysis).

Similarly, a cost metric can be characterized in terms of

- The cyber resiliency strategies or approaches for which it measures effectiveness.
- The type(s) of cost it measures[9].
- How the metric is evaluated (e.g., cost estimation, risk assessment, post hoc analysis).

However, for a metric to be useful in practice, more detailed information is needed. Metrics templates and guidance have been defined for security (NIST, 2008) and operational resilience (Allen, et al., 2010). These templates and guidance, together with the Cyber Resiliency Engineering Framework, were used to create metric templates as shown in Appendix A.

3.2 Metrics

A representative set of cyber resiliency metrics was derived from

[8] The set of approaches currently used by the prototype tool are an earlier version than those in the Cyber Resiliency Engineering Framework. The tool will be updated in FY12.

[9] The Cyber Resiliency Engineering Framework identifies various types of cyber resiliency cost, including life-cycle, mission, support, and opportunity costs, to be considered when deciding whether and how to apply a given cyber resiliency approach.

- The security metrics literature, notably (Herrmann, 2007), (Brotby, 2009), (NIST, 2008), (CIS, 2010).
- Security metrics used by The MITRE Corporation.
- MITRE-internal analyses of resilience characteristics and reviews of the resilience literature, including analyses that produced Version 1.0 of the Cyber Resiliency Engineering Framework (Bodeau and Graubart 2011).
- The growing literature on resilience and resilience metrics, including (AMBER 2009), (ENISA 2011), (Almeida, Madeira and Vieira 2010).
- Discussions with Principal Investigators of cyber resiliency technologies being explored under the MITRE Innovation Program.

Eight technical and eleven cost metric templates were filled in; an example of a completed template is also included in Appendix A. Appendix B presents a representative set of technical metrics, in table form. The table excerpts and summarizes material from the template, identifying for each metric

- An identifier, for quick reference.
- A title, name, or summary definition of the metric.
- Intended use or uses, identifying the types of decisions (operational, engineering, or both) the metric is intended to support.
- Cyber resiliency goals (Anticipate – A, Withstand – W, Recover – R, and/or Evolve – E); an X indicates that the metric can help answer questions about how well the goal is met.
- Cyber resiliency objectives; the metric can help answer questions about how the identified objectives are achieved.
- Cyber resiliency practices; the metric can help answer questions about how effectively the identified practices are applied.
- Layers at which the metric can be evaluated.
- Notes, identifying whether higher or lower values are preferred and assumptions about the environment in which the metric is evaluated.

4 Addressing Issues and Concerns

Cyber resiliency metrics share a variety of issues with security metrics (Brennan, et al., 2009) (Jansen, 2009) (IATAC, 2009), including

- Deficiencies in underlying models. Models underlying metrics definitions include models of network, system, or component behavior and dependencies; of the relationships among objectives and approaches; of adversary strategies and behavior; and of mission dependencies on cyber resources. Models can be incomplete, vague or underspecified, or inconsistent (internally or with related models).
- Mismatches between metrics assumptions and the decision environments in which metrics are used. The description of a metric includes (often implicit) assumptions about the environments in which the metric will be evaluated.
- Use of unspecified, indeterminate, or possibly indeterminate terms in metrics descriptions. Such terms require interpretation. For example, the time an attack starts is indeterminate: what constitutes an attack is a matter for expert judgment, and the actual start of an attack may be impossible to determine. Expert judgments can differ, and in practice metrics evaluation often involves non-experts.
- Inability to establish target values – or even to state whether a given value of a metric is good, bad, or indifferent. A commonly desired use of security metrics is assessment of

compliance (with requirements or with standards of good practice). However, the property motivating the metric definition may be one for which objectives cannot be clearly identified, due to lack of a common body of knowledge. In that case, defining requirements and assessing compliance can be an exercise in fiction rather than engineering.

Additional concerns include:

- Evaluating and tracking metrics requires resources. The benefits – in terms of improved understanding and decision support – of using a metric should outweigh the costs.
- Metrics can be misused, particularly in the context of compliance.
- Metrics can fail to scale easily. Algorithms or models that enable metrics that can feasibly be evaluated at one scale to be combined or "rolled up" to metrics at a larger scale may be lacking or indefensible.
- The tension between what decision-makers want to know, and what can be evaluated in a given technical and/or operational environment, can lead to misinterpretation or deprecation of metrics.

Metrics research in cyber security and resilience may resolve some of the problems with existing metrics. Until research proves out and cyber resiliency engineering is better established as a discipline, these issues and concerns can be addressed in several ways:

- Underlying models for cyber resiliency can be articulated clearly and kept simple. The Cyber Resiliency Engineering Framework constitutes an attempt to do this.
- Metrics descriptions can be annotated to identify underlying models, assumptions, and reasonable uses. The cyber resiliency technical and cost metric templates include a notes section.
- Metrics descriptions can include clear and unambiguous instructions on evaluation, or can be defined as what is produced by an automated tool. However, this benefit is at the cost of relying on metrics that tools can produce, rather than metrics that answer stakeholder questions.
- The usefulness of tracking a metric over time, even without target values, can be emphasized – relative values and trends can be informative. Such tracking is a way to improve understanding and to lead eventually to a body of knowledge based on which target values can be established.
- Metrics already in use (or the data collected for in-use metrics) can be repurposed for cyber resiliency.
- The non-resiliency benefits of evaluating and tracking a metric can be clearly stated. For example, some cyber resiliency metrics assume that mission-essential functions have been identified. That identification is beneficial not only to cyber resiliency engineering, but also to investment planning.
- Metrics can be characterized in terms of their intended uses (either at a high level, as in the distinction between operational and engineering metrics, or with great specificity). One way of characterizing metrics is to distinguish between Measures of Effectiveness (MOEs), Measures of Performance (MOPs), and Technical Performance Measures (TPMs) (INCOSE, 1998) (Campbell, 2004).

5 Directions for Future Work

The representative set could be expanded, by defining cyber resiliency metrics using the Goal-Question-Metric method. In addition, some structure could be applied to the set of metrics, creating a richer knowledge base. For example, metrics that measure the same property at different architectural layers could be identified in relation to a more general (and possibly notional) metric for that property.

Cyber resiliency engineering is a nascent sub-discipline of mission assurance engineering, which is itself in its infancy. Thus, the set of cyber resiliency goals, objectives, and approaches, as well as the ways those approaches can be integrated into an architecture, can be expected to change. The initial representative set of metrics is perforce incomplete, and some metrics may prove infeasible or not worth the effort to evaluate. The set is offered as a starting point, not an end point. The growth of a discipline beyond its pre-paradigm phase is driven by improved understanding[10]. By evaluating and tracking metrics, stakeholders can better understand the cyber resiliency problem domain, appreciate where to focus their attention and efforts, and make decisions.

[10] "Count something." (Gawande, 2007)

Appendix A Templates

Technical Cyber Resiliency Metric Template

Metric Name/Identifier	Name or identifier of base metric; for example, METRIC-TECH-27.
Measurement Description	Describe the attribute being measured; for example, number of resilience requirements for a service.
Metric Use	Describe the intended use(s) of the metric, i.e., the motivating questions it is intended to answer and the stakeholders whose decisions it is intended to support. Questions can be motivated by • Cyber resiliency objectives. (How well is this objective achieved? For example, for the Constrain objective, how effectively has a damage limitation strategy been defined?) • Cyber resiliency approaches. (How effectively is this approach applied? For example, for the Diversity approach, how broadly is diversity applied?) Stakeholders can include • Mission commanders (or business function heads). • Cyber defenders (e.g., CND staff; staff in a Resiliency Operations Center, a Cyber Operations Center, or a Cyber Security Operations Center). • Officials responsible for mission continuity, business continuity, or contingency planning. • Senior IT/ICT providers (e.g., the manager of a data center which provides resources to multiple missions or users, the provider of a common infrastructure such as a network or of a set of shared services such as identity management). • Senior information security or information assurance (IA) staff (e.g., Chief Information Security Officer). • Program managers (as informed by systems engineers and architects). • Architects and systems engineers • Researchers. • Product vendors and solutions providers.
Measurement Scale	• Define the type of scale: nominal, ordinal, cardinal, interval, or ratio. • Define the set of values, or identify the categories, that are valid for the metric: for example, positive whole numbers only, very high to very low. • Define the units.
Intended Use	Describe briefly (e.g., using the terms Operations and/or Engineering) the types of decisions the metric is intended to support. Amplify as appropriate under Metric Use.
How Obtained	Describe briefly (i.e., in a short phrase) how the metric is evaluated. Provide amplifying information under Data Collection and Metric Assessment.
Data Collection and Metric Assessment • How (process) • When/How Often • By Whom (roles, tools)	Describe how the data will be collected and translated into an assessed value of the metric (process), when and how often the data will be collected (event driven, periodic), and who will collect the data (people, tool). Specify whether the collection/assessment method is objective or subjective. Refer to forms or standards if needed.

Data Storage • Where • How • Access Control	Identify where the data is to be stored. Identify the storage media, procedures, and tools for configuration control. Specify how access to this data is controlled.
Aspects of Cyber Resiliency Addressed	Identify which cyber resiliency goals (anticipate, withstand, recover, evolve) and objectives (understand, prevent, prepare, constrain, continue, reconstitute, transform, re-architect) the metric addresses.
Cyber Resiliency Practice (or Practices) Assessed	Identify the cyber resiliency practice (or practices) for which the metric assesses performance.
Architectural Layers / Types of Cyber Resources Addressed	Identify the extent to which the metric applies to an architecture layer (or to a *dependency between layers*) in the notional layered architecture, or to a specified set of cyber resources (applies, applies partially or with interpretation, does not apply). Notional layers include: • Organization • *Organization/Mission Dependency* • Mission or Line of Business • *Mission/Process Dependency* • Mission or Business Process • *Process/Support Dependency* • Support for Mission Task or Capability • *Support/Asset Dependency* • Information Asset • *Asset/Node Dependency* • Node
Notes	Provide any notes that might be helpful in interpreting or using the metric.

Cyber Resiliency Cost Metric Template

Metric Name/Identifier	Name or identifier of base metric; for example, METRIC-COST-3.
Measurement Description	Describe the attribute being measured; for example, dollar cost of acquiring a new resiliency technology.
Metric Use	Describe the intended use of the metric, i.e., the motivating questions it is intended to answer and/or the types of decisions the metric is intended to support. Examples of motivating questions include: What is the LOE cost of employing new technology? What is the dollar cost of maintaining resiliency technology? What is the impact of incorporating resiliency technology? Examples of decisions include acquisition, maintenance, de-acquisition, and transition investment.
Measurement Scale	• Define the type of scale: nominal, ordinal, cardinal, interval, or ratio • Define the set of values, or identify the categories, that are valid for the metric: for example, positive whole numbers only, very high to very low. • Define the units: for example, dollar cost, level-of-effort cost, degree of impact.
Cyber Resiliency Approaches	Identify the cyber resiliency approaches to which the cost metric is relevant.
How Obtained	Describe briefly (i.e., in a short phrase) how the metric is evaluated (e.g., cost estimation, analysis of actual expenditures). Provide amplifying information under Data Collection and Metric Assessment.
Life-Cycle Costs Addressed?	Identify whether the metric addresses life-cycle costs (yes, no, partially; if partially, describe how in the Notes on Aspects of Cost Addressed).
Support Costs Addressed?	Identify whether the metric addresses support costs (yes, no, partially; if partially, describe how in the Notes on Aspects of Cost Addressed).
Consequential Costs and Benefits Addressed?	Identify whether the metric addresses consequential costs and Benefits (yes, no, partially; if partially, describe how in the Notes on Aspects of Cost Addressed).
Notes on Aspects (L, S, C) of Cost Addressed	Provide additional information on the extent to which the metric addresses aspects of cost. If more than one aspect is addressed, indicate relative extent, such as primarily or secondarily, if there is a discernible difference.
Data Collection and Metric Assessment • How • When/How Often • By Whom	Describe how the data will be collected and translated into an assessed value of the metric (process), when and how often the data will be collected (event driven, periodic), and who will collect the data (people, tool). Specify whether the collection/assessment method is objective or subjective. Refer to forms or standards if needed.
Data Storage • Where • How • Access Control	Identify where the data is to be stored. Identify the storage media, procedures, and tools for configuration control. Specify how access to this data is controlled.
Architectural Layers Addressed	Identify the types of cyber resources and/or the architectural layers (from the notional layered architecture) to which the cost metric is relevant.
Notes	Provide any notes that might be helpful in interpreting or using the metric.

Example: Completed Cost Metric Template

Metric Name/Identifier	METRIC-COST-1
Measurement Description	Dollar cost of acquiring new resiliency technology
Metric Use	Support decisions affecting the acquisition of resiliency technology. Cost of new technology is one factor in a trade-off analysis (e.g., cost-benefit analysis).
Measurement Scale	• Scale: ratio • Units: dollars
Strategy	Adaptive Response, Deception, Diversity, Dynamic Positioning, Segmentation, Unpredictability, and Validation
How Obtained	• Cost estimation • Analysis of actual expenditures
Life-Cycle Costs Addressed?	Yes
Support Costs Addressed?	No
Consequential Costs and Benefits Addressed?	No
Notes on Aspects (L, S, C) of Cost Addressed	This metric addresses only the initial cost of the new resiliency technology; a separate metric addresses the cost of maintaining it.
Data Collection and Metric Assessment • How • When/How Often • By Whom	Cost estimation is done as part of the system engineering process on a one-time basis. Actual expenditures are reported by acquisition personnel.
Data Storage • Where • How • Access Control	These factors, when relevant to the use of this metric, should be determined by the analysts using this metric.
Architectural Layers Addressed	This metric primarily addresses the following architectural layers: • Support for Mission Task or Capability • Information Asset • Node
Notes	None

Appendix B Representative Set of Cyber Resiliency Metrics

Metric Identifier	Summary Definition	Intended Use	Goal(s)				Objective(s)	Practice(s)	Layer(s)	Notes
			A	W	R	E				
METRIC-TECH-1	Percentage of cyber resources that are properly configured	Operations	X				Prepare	Coordinated Defense	Cyber resource (system-of-systems)	Higher values are better. It assumes that the organization evaluating it (1) has defined the scope of "cyber resources" (e.g., systems in a system-of-systems, clients and servers in an enclave), (2) has established what it means for cyber resources to be properly configured or hardened, and (3) has a means to determine whether a cyber resource is properly configured or hardened. For an example of how to specify this metric, see CIS, Percent of Systems Without Known Severe Vulnerabilities.
METRIC-TECH-2	Number of attempted intrusions stopped at a network perimeter	Operations and Engineering	X	X			Prevent, Continue	Coordinated Defense	Cyber resource (network)	Higher values are better. This metric assumes (1) an established definition of attempted intrusion, (2) a means to count attempted intrusions stopped at the perimeter and attempted intrusions not stopped at the perimeter, and (3) a time period for which the metric is evaluated (either in an operational environment or in a test / simulation environment to support engineering analysis). If the metric is evaluated in a test / simulation environment, “percentage” rather than “number” can be used.
METRIC-TECH-4	Number of attempted intrusions deflected to a honeypot	Operations and Engineering	X	X			Prevent, Continue	Deception	Cyber resource (network)	Higher values are better. This metric assumes (1) an established definition of attempted intrusion, (2) a means to count attempted intrusions deflected to a deception environment and attempted intrusions deflected, and (3) a time period for which the metric is evaluated (either in an operational environment or in a test / simulation environment to support engineering analysis). It also assume that a deception environment is established and maintained. If the metric is evaluated in a test / simulation environment, “percentage” rather than “number” can be used.
METRIC-TECH-6	Length of time between an initial adversary act and its detection	Operations	X				Prevent	Coordinated Defense	Cyber resource (system / network)	Lower values are better. This metric assumes that the initial adversary act can be identified, making the metric most meaningful in a test / simulation / Red Team environment.

Metric Identifier	Summary Definition	Intended Use	Goal(s)				Objective(s)	Practice(s)	Layer(s)	Notes
			A	W	R	E				
METRIC-TECH-7	Percentage of mission-essential functions for which a procedural work-around is available	Operations		X			Continue	Diversity	Mission process	Higher values are better. This metric assumes that mission-essential functions have been identified, and a means for determining whether a procedural work-around is available. (Note that documentation of a procedural work-around may not suffice for the work-around to be available; for example, a procedural work-around could assume that staff with specific expertise are present, and such staff could only be present on a single shift.)
METRIC-TECH-8	Percentage of mission-essential capabilities for which two or more different instantiations are available	Engineering		X			Continue	Diversity	Mission process, Cyber resource (service)	Higher values are better. This metric assumes (1) that mission-essential capabilities (i.e., ability to accomplish a mission essential task, which may be identified with cyber resources such as services) have been identified, (2) a means for determining whether a two or more instantiations are different, and (3) a means for determining whether an instantiation is available.
METRIC-TECH-10	Additional / diverted level of effort to maintain mission-essential functions	Operations		X			Continue	Adaptive Response	Mission process, Personnel	Lower values are better. This metric, which assesses the effectiveness of resiliency solutions, can also be viewed as a cost metric. It assumes that the LOE needed to maintain mission-essential functions during an attack can be determined (e.g., by identifying which staff are dedicated to maintaining mission-essential functions and by comparing the actual hours logged to the planned hours).
METRIC-TECH-12	Degree of degradation of mission-essential functions	Operations		X			Continue	Adaptive Response	Mission process	Lower values are better. This is actually a set of metrics (or, alternately, the average, median, or maximum of that set), one for each mission-essential function. This metric assumes that (1) mission-essential functions have been identified, (2) the expected level of performance for each mission-essential function has been specified (e.g., using SLAs or KPPs), and (3) a means has been defined for evaluating the level of performance.

Metric Identifier	Summary Definition	Intended Use	Goal(s)				Objective(s)	Practice(s)	Layer(s)	Notes
			A	W	R	E				
METRIC-TECH-13	Length of time between initial disruption and availability (at minimum level of acceptability) of mission-essential functions	Operations		X	X		Continue	Adaptive Response	Mission process	Lower values are better. This is actually a set of metrics (or, alternately, the average, median, or maximum of that set), one for each mission-essential function. This metric assumes that (1) mission-essential functions have been identified, (2) the minimum level of performance for each mission-essential function has been specified (e.g., using SLAs or KPPs), (3) a means has been defined for evaluating the level of performance, and (4) the times when the initial disruption occurred and when each mission-essential function achieved its minimum acceptable level can be determined.
METRIC-TECH-14	Percentage of mission-essential datasets for which all items effectively have two or more independent external data feeds	Engineering		X	X		Continue, Reconstitute	Diversity	Information asset (information store)	Higher values are better. This is actually a set of metrics (or, alternately, the average, median, or maximum of that set), one for each mission-essential data store. This metric assumes that (1) mission-essential data stores have been identified, (2) what constitutes an item (e.g., a data value assertion such as a single numerical value in a relation, a data object containing multiple data values such as an image) has been defined, (3) whether an item has two or more external data feeds can be determined, and (4) what it means for two data feeds to be independent has been defined. For this metric to be evaluated, METRIC-TECH-15 must be evaluated for each data store.
METRIC-TECH-15	Percentage of data value assertions in a mission-essential data store for which two or more different data feeds are available	Engineering		X	X		Continue, Reconstitute	Diversity	Information asset (information store)	Higher values are better. This metric assumes that (1) a data store has been identified as mission-essential, (2) what constitutes an item (e.g., a data value assertion such as a single numerical value in a relation, a data object containing multiple data values such as an image) has been defined, (3) whether an item has two or more external data feeds can be determined, and (4) what it means for two data feeds to be independent has been defined.

Metric Identifier	Summary Definition	Intended Use	Goal(s)				Objective(s)	Practice(s)	Layer(s)	Notes
			A	W	R	E				
METRIC-TECH-16	Percentage of mission-essential data stores for which a master copy exists	Engineering		X	X		Continue, Reconstitute	Substantiated Integrity	Information asset (information store)	Higher values are better. This metric assumes that (1) mission-essential data stores have been identified, (2) what constitutes a gold copy has been defined, and (3) a means for determining the existence of a gold copy has been defined.
METRIC-TECH-17	Percentage of data value assertions in a mission-essential data store for which a master copy exists	Engineering		X	X		Continue, Reconstitute	Substantiated Integrity	Information asset (information store)	Higher values are better. This metric assumes that (1) a data store has been identified as mission-essential, (2) what constitutes an item (e.g., a data value assertion such as a single numerical value in a relation, a data object containing multiple data values such as an image) has been defined, (3) what constitutes a gold copy of an item has been defined, and (4) what it means for determining the existence of a gold copy has been defined.
METRIC-TECH-18	Additional / diverted level of effort to restore operation	Operations			X		Reconstitute	Adaptive Response	Mission process, Personnel	Lower values are better. This metric, which assesses the effectiveness of resiliency solutions, can also be viewed as a cost metric. It assumes that the LOE needed to restore normal operations after an attack can be determined (e.g., by identifying which staff are dedicated to maintaining mission-essential functions and by comparing the actual hours logged to the planned hours).
METRIC-TECH-20	Length of time between initial disruption and restoration	Operations and Engineering		X	X		Continue, Reconstitute	Adaptive Response	Mission process	Lower values are better. This metric assumes that (1) the time of the initial disruption can be determined, (2) capabilities have been identified, and (3) capabilities can be fully restored.
METRIC-TECH-21	Percentage of pre-disruption availability / performance after disruption	Operations			X		Continue	Adaptive Response	Mission process	Higher values are better. This metric assumes that (1) the time of the initial disruption can be determined, (2) capabilities have been identified, and (3) the level of performance or availability for each capability can be assessed.
METRIC-TECH-22	Quality of restored / recovered / reconstituted data	Operations and Engineering			X		Continue, Reconstitute	Redundancy, Substantiated Integrity	Information asset (information store)	Higher values are better. This metric assumes that (1) levels of data quality have been defined and (2) ways of evaluating data quality have been established.

Metric Identifier	Summary Definition	Intended Use	Goal(s)				Objective(s)	Practice(s)	Layer(s)	Notes
			A	W	R	E				
METRIC-TECH-24	Percentage of data irrevocably lost	Operations and Engineering			X		Continue, Reconstitute	Redundancy, Substantiated Integrity	Information asset (information store)	Lower values are better. This metric assumes a clear definition of what it means for data to be lost, e.g., data has been corrupted or deleted and cannot be reliably reconstructed from backups or other data stores.
METRIC-TECH-26	Percentage of systems redesigned to improve damage limitation	Engineering				X	Re-architect	Security Engineering	Cyber resource (system-of-systems)	Higher values are better. This metric assumes that (1) systems can be clearly identified, (2) systems can be redesigned to improve damage limitation, and (3) a starting point or time period for evaluating the metric is established (e.g., systems redesigned in the past three years, systems redesigned since IOC).
METRIC-TECH-27	Number of new sensors installed	Operations and Engineering	X			X	Prepare, Re-architect	Analytic Monitoring, Security Engineering	Cyber resource (system-of-systems)	Higher values are better. This metric assumes that a starting point or time period for evaluating the metric is established (e.g., sensors or capabilities installed in the past three months, sensors or capabilities installed during the current evolutionary spiral).
METRIC-TECH-29	Length of time to deploy redundant resources	Engineering	X	X			Prepare, Continue	Coordinated Defense, Redundancy	Cyber resource	Lower values are better. This metric assumes that (1) redundant resources exist, (2) the time when the decision to deploy redundant resources in the operational environment can be determined, (3) what it means for a resource to be successfully deployed is defined, and (4) the time when a resource has been successfully deployed can be determined.
METRIC-TECH-31	Length of time to deploy a new instantiation of a required capability	Operations		X			Continue	Diversity	Cyber resource	Lower values are better. This metric assumes that (1) required capabilities have been identified, (2) what constitutes a new instantiation of a capability has been defined, (3) the time when the decision to deploy a new instantiation in the operational environment can be determined, (4) what it means for a capability to be successfully deployed is defined, and (5) the time when a resource has been successfully deployed can be determined.
METRIC-TECH-33	Number of alternate instantiations of a required capability that can be deployed	Operations		X			Continue	Diversity	Cyber resource	Higher values are better. This metric assumes that (1) required capabilities have been identified, and (2) what constitutes an alternative instantiation of a capability has been defined.

Metric Identifier	Summary Definition	Intended Use	Goal(s)				Objective(s)	Practice(s)	Layer(s)	Notes
			A	W	R	E				
METRIC-TECH-35	Average length of time between the start of adversary acts and their discovery	Operations	X				Prevent	Coordinated Defense	Cyber resource (system / network)	Lower values are better. This common security metric assumes a consistent method for identifying (1) when an incident begins and (2) when an incident is discovered. It also assumes a time period during which incidents are observed (e.g., average length of time during the first calendar quarter; average length of time from [specified date] to the present).
METRIC-TECH-37	Average length of time to recover from incidents	Operations			X		Reconstitute	Adaptive Response	Cyber resource (system / network)	Lower values are better. This common security metric assumes a consistent method for identifying (1) when an incident begins and (2) when incident recovery is complete. It also assumes a time period during which incidents (and recovery from incidents) are observed (e.g., average length of time during the first calendar quarter; average length of time from [specified date] to the present). For an example of how to specify this metric, see CIS, Mean-Time to Incident Recovery.
METRIC-TECH-38	Average length of time to patch systems	Operations	X				Prevent	Coordinated Defense	Cyber resource (system / network)	Lower values are better. This metric assumes that systems have been identified. For an example of how to specify this metric, see CIS, Mean Time to Patch.
METRIC-TECH-41	Average length of time to patch network components	Operations	X				Prevent	Coordinated Defense	Cyber resource (system / network)	Lower values are better. This metric assumes that networking components have been identified. For an example of how to specify this metric, see CIS, Mean Time to Patch.
METRIC-TECH-39	Percentage of systems in compliance with organizationally mandated configuration guidance	Operations	X				Prevent	Coordinated Defense	Cyber resource (system / network)	Higher values are better. This metric assumes that systems have been identified and configuration requirements have been specified. For an example of how to specify this metric, see CIS, Percentage of Configuration Compliance.
METRIC-TECH-40	Percentage of information system security personnel that have received security training	Operations	X				Prepare	Coordinated Defense	Org processes, Personnel	Higher values are better. This metric assumes that resilience-aware security training (i.e., training that includes responsibilities and processes for coordination as part of security management / administration and security operations) has been established. For an example of how to specify this metric, see NIST SP 800-55, Measure 4: Awareness and Training.

Metric Identifier	Summary Definition	Intended Use	Goal(s)				Objective(s)	Practice(s)	Layer(s)	Notes
			A	W	R	E				
METRIC-TECH-42	Frequency of audit record analysis for inappropriate activity	Operations	X				Understand	Analytic Monitoring	Cyber resource (system / network), Personnel	Higher values are better. This metric assumes that criteria for inappropriate activity have been established. For an example of how to specify this metric, see NIST SP 800-55, Measure 5: Audit and Accountability.
METRIC-TECH-44	Percentage of information systems for which annual testing of contingency plans has been conducted	Operations	X				Prepare	Coordinated Defense, Security Management	Org processes, Cyber resource (system)	Higher values are better. Note that, to support cyber resiliency, contingency plans should take into consideration the cyber threat. For an example of how to specify this metric, see NIST SP 800-55, Measure 8: Contingency Planning.
METRIC-TECH-46	Percentage of incidents reported within required timeframe per applicable incident category	Operations	X	X			Understand	Analytic Monitoring	Org processes	Higher values are better. This metric assumes that (1) what constitutes an incident has been defined, (2) incident categories have been established, and (3) a required timeframe for incident reporting has been established. For an example of how to specify this metric, see NIST SP 800-55, Measure 10: Incident Response.
METRIC-TECH-47	Average length of time between the occurrence and the discovery of an anomaly	Operations	X	X			Understand, Continue	Analytic Monitoring, Coordinated Defense	Org processes	Lower values are better. This common security metric assumes a consistent method for (1) defining what constitutes an anomaly, (2) identifying when an anomaly occurs, and (3) when an anomaly is discovered. It also assumes a time period during which incidents are observed (e.g., average length of time during the first calendar quarter; average length of time from [specified date] to the present).
METRIC-TECH-49	Average length of time between cyber incidents	Operations	X	X			Understand	Analytic Monitoring	Cyber resource (system / network)	Lower values are better. This common security metric assumes a consistent method for (1) defining what constitutes an incident and (2) identifying when an incident occurs. It also assumes a time period during which incidents are observed (e.g., average length of time during the first calendar quarter; average length of time from [specified date] to the present).

Metric Identifier	Summary Definition	Intended Use	Goal(s)				Objective(s)	Practice(s)	Layer(s)	Notes
			A	W	R	E				
METRIC-TECH-53	Average length of time for the organization to recover from damage caused by a cyber incident	Operations			X		Reconstitute	Adaptive Response	Org processes, Cyber resource (system / network)	Lower values are better. This metric assumes that (1) what constitutes an incident is defined, (2) the time when an incident starts can be determined, and (3) the time when recovery is complete can be determined. It also assumes a time period during which incidents are observed (e.g., average length of time during the first calendar quarter; average length of time from [specified date] to the present).
METRIC-TECH-55	Percentage of managed systems checked for vulnerabilities in accordance with the organization's policy	Operations	X				Prevent	Coordinated Defense	Cyber resource (system)	Higher values are better. This metric assumes that (1) managed systems have been identified, and (2) a specified frequency and/or a specified time period after the mechanism for checking has been deployed has been established. For an example of how to specify this metric, see CIS, Vulnerability Scanning Coverage.
METRIC-TECH-56	Percentage of systems without “high” severity vulnerabilities based on Common Vulnerability Scoring System (CVSS) scoring	Operations	X				Prevent	Coordinated Defense	Cyber resource (system)	Higher values are better. This metric assumes that (1) systems have been identified and (2) systems can be scanned for vulnerabilities. For an example of how to specify this metric, see CIS, Percent of Systems with No Known Severe Vulnerabilities.
METRIC-TECH-57	Average length of time for the organization to mitigate identified vulnerabilities	Operations	X				Prevent	Coordinated Defense	Org processes	Lower values are better. This metric assumes that (1) cyber resources (e.g., systems, applications) with vulnerabilities have been identified and (2) vulnerabilities can be mitigated. For an example of how to specify this metric, see CIS, Mean Time to Mitigate.
METRIC-TECH-58	Percentage of managed systems for which an automated patch management process is used	Operations and Engineering	X				Prevent	Coordinated Defense	Cyber resource (system)	Higher values are better. This metric assumes that (1) technologies (e.g., operating systems, applications) have been identified and (2) a patch management process can be defined. For an example of how to specify this metric, see CIS, Patch Management Coverage.

Metric Identifier	Summary Definition	Intended Use	Goal(s)				Objective(s)	Practice(s)	Layer(s)	Notes
			A	W	R	E				
METRIC-TECH-60	Average length of time from patch release to patch installation	Operations	X				Prevent	Coordinated Defense	Org processes, Cyber resource (system)	Lower values are better. This metric assumes a definition of what it means for patch installation to be complete (e.g., 98% of all systems for which the patch is required). This metric also assumes a time period during which incidents are observed (e.g., average length of time during the first calendar quarter; average length of time from [specified date] to the present). For an example of how to specify this metric, see CIS, Mean Time to Patch.
METRIC-TECH-62	Percentage of systems for which a defined security configuration is required	Engineering	X				Prevent	Coordinated Defense	Cyber resource (system)	Higher values are better. This metric assumes that systems have been identified, and is most relevant for an organization with a heterogeneous set of systems.
METRIC-TECH-63	Percentage of personnel who successfully completed annual security training	Operations	X				Prevent	Security Management	Org processes	Higher values are better. This metric recognizes that end users play a role in cyber defense.
METRIC-TECH-65	Percentage of enterprise considered to be monitored effectively	Operations and Engineering	X				Understand	Analytic Monitoring	Cyber resource (system / network)	Higher values are better. This metric assumes that (1) enterprise cyber resources have been defined and identified and (2) what constitutes effective monitoring has been defined.
METRIC-TECH-83	Class of attacks that can be detected with existing means	Operations and Engineering	X	X			Understand	Analytic Monitoring	Cyber resource (system / network)	Higher values are better. This metric assumes that (1) classes of attacks are sufficiently well-defined that an attack or incident can be assigned to a class and (2) the classes of attacks relevant to the mission / business function or organization have been determined.
METRIC-TECH-85	Percentage of individually managed systems having a defined mode for degraded operation	Operations and Engineering	X	X			Prevent, Continue	Adaptive Response, Coordinated Defense	Cyber resource (system / network)	Higher values are better. This metric assumes that (1) individually managed systems are defined and identified, (2) what "the capability to operate in a degraded mode" means is well-defined, and (3) a consistent method for determining whether a system is capable of operating in a degraded mode can be defined.

Metric Identifier	Summary Definition	Intended Use	Goal(s)				Objective(s)	Practice(s)	Layer(s)	Notes
			A	W	R	E				
METRIC-TECH-86	Percentage of individually managed systems in which one or more resiliency techniques have been implemented	Operations and Engineering	X	X			Prevent, Continue	Adaptive Response, Coordinated Defense	Cyber resource (system / network)	Higher values are better. This metric assumes that (1) individually managed systems are defined and identified, (2) what it means for a cyber resiliency technique to be implemented in a system is well-defined, and (3) a consistent method for determining whether a resiliency technique has been implemented in a system can be defined.
METRIC-TECH-89	Percentage of mission-essential processes and interfaces restored to pre-disruption state	Operations			X		Reconstitute	Adaptive Response	Cyber resource (system / network)	Higher values are better. This metric assumes that (1) mission-essential processes and interfaces have been defined and (2) whether a process or interface has been restored to its pre-disruption state can be determined.
METRIC-TECH-90	Level of trust in a system that has been restored to its pre-disruption capability	Operations and Engineering			X		Reconstitute	Adaptive Response	Cyber resource (system)	Higher values are better. This metric assumes that (1) levels of trust have been defined and (2) whether a system has been restored to its pre-disruption state can be determined. This metric recognizes that a system that has been restored to its pre-disruption state in terms of functionality could still be compromised.
METRIC-TECH-92	Quality of choices made during design and engineering that affect resiliency	Engineering				X	Re-architect	Adaptive Response	Org processes, Cyber resource (system / network)	Higher values are better. This metric assumes that (1) criteria and processes for considering resiliency as part of design and engineering decisions have been established and (2) decisions can be identified and evaluated against those criteria.
METRIC-TECH-95	Degree of consistency between organizational threat-response policies for system managers and organizational threat-response policies for operators	Operations	X				Prepare	Coordinated Defense	Org processes	Higher values are better. This metric assumes that (1) threat-response policies and procedures for system managers and operators exist and (2) criteria for assessing consistency can be defined.
METRIC-TECH-96	Percentage of network and operations managers maintaining an organizationally-defined acceptable level of risk management skills	Operations	X				Prepare	Security Management	Org processes	Higher values are better. This metric assumes that an acceptable level of risk management skills for network managers and operators can be defined.

Metric Identifier	Summary Definition	Intended Use	Goal(s)				Objective(s)	Practice(s)	Layer(s)	Notes
			A	W	R	E				
METRIC-TECH-97	Percentage of network and operations managers maintaining an organizationally-defined acceptable level of threat awareness	Operations	X				Prepare	Security Management	Org processes	Higher values are better. This metric assumes that an acceptable level of threat awareness for network managers and operators can be defined.
METRIC-TECH-98	Degree to which system operators deviate from documented cyber resiliency guidance and procedures	Operations	X				Prepare	Security Management	Org processes	Lower values are better. This metric assumes that cyber resiliency guidance and procedures for system operators have been documented.
METRIC-TECH-99	Quality of documentation on system operation	Operations	X				Prepare	Security Management	Org processes	Higher values are better. This metric assumes that criteria for assessing the quality (e.g., completeness, consistency with actual technologies, consistency with mission / business process documentation or practice) of system operation documentation have been defined.
METRIC-TECH-100	Confidence level in the reliability of electrical power for mission support systems	Engineering	X				Prepare	Coordinated Defense	Facilities	Higher values are better. The level of confidence is typically determined as part of contingency planning. This metric assumes that (1) mission support systems have been identified, and (2) criteria for assessing the reliability of the power source(s) for mission support systems have been defined.
METRIC-TECH-101	Percentage of red team attack scenarios where varying configurations of interrelated functions are subjected to attack	Operations and Engineering		X			Understand, Continue	Substantiated Integrity	Org processes, Cyber resource (system)	Higher values are better. This metric assumes that red team activities are used to evaluate the cyber security posture.
METRIC-TECH-114	Percentage of security components that are monitored for communication between an adversary and their implanted malicious code	Operations	X				Understand	Analytic Monitoring	Cyber resource (system)	Higher values are better. This metric assumes that (1) what constitute security components are defined and (2) security components are identified. Examples of security components include firewalls, Domain Name Service (DNS)/Active Directory (AD), Network Intrusion Detection Systems (NIDS)/ Intrusion Prevention Systems (IPS), and Local Area Network (LAN) equipment.

Metric Identifier	Summary Definition	Intended Use	Goal(s)				Objective(s)	Practice(s)	Layer(s)	Notes
			A	W	R	E				
METRIC-TECH-115	Percentage of mission critical components that employ anti-tamper, shielding, and power line filtering	Engineering	X	X			Understand, Continue, Constrain	Substantiated Integrity, Segmentation	Cyber resource (system)	Higher values are better. This metric assumes that mission-critical components have been identified.
METRIC-TECH-117	Percentage of mission critical components that are purpose built	Operations and Engineering	X	X			Understand, Continue	Substantiated Integrity	Cyber resource (system / network)	Higher values are better. This metric assumes that mission-critical components have been identified.
METRIC-TECH-121	Level of access limitation for external maintenance personnel	Operations	X				Understand	Privilege Restriction	Org processes, Facilities	Higher values are better. This metric assumes that levels of access limitation have been defined, based on such considerations as clearance, whether employment has been verified, and whether maintenance personnel are escorted.
METRIC-TECH-123	Percentage of administrators who can administer both network and security components	Operations	X				Understand, Prevent	Substantiated Integrity, Privilege Restriction	Org processes, Cyber resource (system / network)	Lower values are better.
METRIC-TECH-127	Percentage of Network Intrusion Detection Systems that are connected to the network using passive taps	Operations	X				Understand	Analytic Monitoring	Cyber resource (system / network)	Higher values are better.
METRIC-TECH-129	Percentage of Network Intrusion Detection Systems that use an out-of-band network for remote management	Operations	X				Understand, Prevent	Analytic Monitoring, Segmentation	Cyber resource (system / network)	Higher values are better.
METRIC-TECH-131	Number or percentage of Network Intrusion Detection Systems that are implemented on separate platforms	Operations	X	X			Prevent, Continue	Analytic Monitoring, Segmentation	Cyber resource (network)	Higher values are better.
METRIC-TECH-132	Length of time to bring online a backup network intrusion detection system	Operations	X	X			Understand, Continue	Analytic Monitoring, Redundancy	Cyber resource (network)	Lower values are better. This metric assumes that a backup network intrusion detection system is available, and that the time from when the decision to bring it online and the time when it is online can be measured.

Metric Identifier	Summary Definition	Intended Use	Goal(s)				Objective(s)	Practice(s)	Layer(s)	Notes
			A	W	R	E				
METRIC-TECH-133	Length of time packet capture and sniffing devices are connected to the network	Operations	X	X			Prevent, Continue	Non-persistence	Cyber resource (network)	Lower values are better. This metric assumes that (1) to mitigate supply chain risks, packet capture and sniffing devices should be connected to the network only when needed; and (2) use of these devices is tracked. This metric also assumes a time period over which it is evaluated.
METRIC-TECH-134	Percentage of DNS servers under the organization's control that have been hardened	Operations	X				Prevent	Coordinated Defense	Cyber resource (system / network)	Higher values are better. Hardening is in accordance with NIST Special Publication 800-81, Secure Domain Name System (DNS) Deployment Guide.
METRIC-TECH-135	Percentage of enterprise DNS servers to which Domain Name System Security (DNSSEC) extensions have been applied	Operations	X				Prevent	Coordinated Defense	Cyber resource (system / network)	Higher values are better.
METRIC-TECH-136	Percentage of local enclaves configured with a DNS server	Operations		X			Continue	Redundancy	Cyber resource (system / network)	Higher values are better.
METRIC-TECH-137	Number of platforms on which multiple DNS servers are co-hosted	Operations		X			Continue	Redundancy	Cyber resource (system / network)	Lower values are better.
METRIC-TECH-138	Percentage of enterprise Active Directory servers that have hot swappable power supplies	Operations		X			Continue	Redundancy	Cyber resource (system / network)	Higher values are better. This metric assumes an enterprise architecture that depends on Active Directory.
METRIC-TECH-139	Percentage of enterprise Active Directory servers that use RAID (Redundant Array of Independent Disks) drives	Operations		X			Continue	Redundancy	Cyber resource (system / network)	Higher values are better. This metric assumes an enterprise architecture that depends on Active Directory.
METRIC-TECH-140	Frequency at which Active Directory is replicated when configured to use multi-master replication	Operations		X			Continue	Redundancy	Cyber resource (system / network)	Higher values are better. This metric assumes an enterprise architecture that depends on Active Directory.

Metric Identifier	Summary Definition	Intended Use	Goal(s)				Objective(s)	Practice(s)	Layer(s)	Notes
			A	W	R	E				
METRIC-TECH-141	Percentage of data centers across which Active Directory domain controllers are distributed where multi-master replication is used	Operations		X			Continue	Redundancy	Cyber resource (system / network)	Higher values are better. This metric assumes an enterprise architecture that depends on Active Directory.
METRIC-TECH-142	Length of time to bring online an Active Directory warm backup domain controller	Operations		X			Continue	Redundancy	Cyber resource (system / network)	Lower values are better. This metric assumes an enterprise architecture that depends on Active Directory. This metric assumes that an Active Directory backup is available, and that the time from when the decision to bring it online and the time when it is online can be measured.
METRIC-TECH-143	Length of time to provide alternate email, file, and instant messaging service when the Active Directory (AD) authenticated services are disrupted	Operations		X			Continue	Redundancy	Cyber resource (system / network)	Lower values are better. This metric assumes an enterprise architecture that depends on Active Directory. This metric assumes that alternative email, file, and instant messaging services are available, and that the time from when the decision to bring them online and the time when they are online can be measured.
METRIC-TECH-144	Percentage of the alternate email, file, and instant messaging services (response to AD denial) that are hosted on an OS platform other than Windows	Operations		X			Continue	Redundancy, Diversity	Cyber resource (system / network)	Higher values are better. This metric assumes an enterprise architecture that depends on Active Directory, but that accommodates OS diversity.
METRIC-TECH-151	Length of time for anomalous or malicious activity to be reported to an operator's console	Operations		X			Understand	Analytic Monitoring	Cyber resource (system / network)	Lower values are better. This metric assumes that criteria for characterizing events or behavior as anomalous or malicious have been established.
METRIC-TECH-152	Percentage of anomalous or malicious events / behavior that can be associated with a person and a computing / communications device	Operations	X	X			Understand	Analytic Monitoring	Cyber resource (system), Personnel, Hardware	Higher values are better. This metric assumes that criteria for characterizing events or behavior as anomalous or malicious have been established.
METRIC-TECH-158	Number of alerts generated when routers or proxies detect attempts to send packets directly to a hidden client	Operations		X			Understand	Analytic Monitoring	Cyber resource (system / network)	The number should be at least one, but should not be so large as to overwhelm the operator; this upper bound needs to be established for the specific operational environment. A hidden client is one whose IP address is not advertised.

Metric Identifier	Summary Definition	Intended Use	Goal(s)				Objective(s)	Practice(s)	Layer(s)	Notes
			A	W	R	E				
METRIC-TECH-159	Length of time to bring a backup server online	Operations			X		Reconstitute	Redundancy	Cyber resource (system)	Lower values are better.
METRIC-TECH-160	Length of time for detailed information about a system to be delivered to an operator who has requested it in response to an alert	Operations		X	X		Understand	Analytic Monitoring	Cyber resource (system)	Lower values are better. This metric assumes that (1) the time when the operator receives the alert can be determined and (2) the time when the operator accesses detailed information can be determined.
METRIC-TECH-176	Length of time to report packets to/from an invalid port on a server	Operations	X	X			Understand	Analytic Monitoring	Cyber resource (system / network)	Lower values are better. This metric assumes that (1) the time at which a packet to or from an invalid port on a server is received or sent can be determined, and (2) the time when the event is reported can be determined.
METRIC-TECH-177	Length of time to report attempts to access unauthorized ports or inaccessible addresses	Operations	X	X			Understand	Analytic Monitoring	Cyber resource (system / network)	Lower values are better. This metric assumes that (1) the time at which an access attempt to an unauthorized port or an inaccessible address is detected can be determined, and (2) the time when the event is reported can be determined.
METRIC-TECH-178	Length of time to report attempts at IP address spoofing	Operations	X	X			Understand	Analytic Monitoring	Cyber resource (system / network)	Lower values are better. This metric assumes that (1) the time at which an attempt at IP address spoofing occurs can be determined, and (2) the time when the event is reported can be determined.
METRIC-TECH-179	Length of time for packets to unroutable IP addresses to be reported	Operations	X	X			Understand	Analytic Monitoring	Cyber resource (system / network)	Lower values are better. . This metric assumes that (1) the time at which packets to unroutable IP addresses are detected can be determined, and (2) the time when the event is reported can be determined.
METRIC-TECH-180	Length of time for packets to/from an invalid port on a server to be reported	Operations	X	X			Understand	Analytic Monitoring	Cyber resource (system / network)	Lower values are better. This metric assumes that (1) the time at which packets to or from an invalid port on a server are detected can be determined, and (2) the time when the event is reported can be determined.
METRIC-TECH-181	Percentage of unauthorized changes to row data in a database that are detected	Operations		X			Understand, Continue, Constrain	Substantiated Integrity, Analytic Monitoring	Information store	Higher values are better.

Metric Identifier	Summary Definition	Intended Use	Goal(s)				Objective(s)	Practice(s)	Layer(s)	Notes
			A	W	R	E				
METRIC-TECH-183	Frequency at which key information assets are replicated to a backup data store or standby system through database journaling	Operations			X		Reconstitute	Redundancy	Information store	Higher values are better. The metric assumes that key information assets are identified.
METRIC-TECH-184	Length of time to reconstitute a key information asset from a backup data store	Operations			X		Reconstitute	Redundancy	Information store	Lower values are better. The metric assumes that key information assets are identified.
METRIC-TECH-189	Length of time to locate tools, services, and data sources needed to repair or reconstitute an infrastructure that serves mission requirements	Operations			X		Reconstitute	Adaptive Response	Software, Information store, Information feed	Lower values are better.
METRIC-TECH-192	Length of time to combine tools, services, and data sources needed to repair or reconstitute the infrastructure that serves mission requirements	Operations			X		Reconstitute	Adaptive Response	Software, Information store, Information feed	Lower values are better.
METRIC-TECH-195	Length of time to put into operational use the tools, services, and data sources needed to repair or reconstitute the infrastructure that serves mission requirements	Operations		X			Reconstitute	Adaptive Response	Software, Information store, Information feed	Lower values are better.
METRIC-TECH-202	Percentage of virtual machine (VM) images available for download for which alternative codebases exist	Operations	X				Understand, Prevent	Unpredictability, Non-persistence, Diversity	Software	Higher values are better.
METRIC-TECH-216	Length of time to change a software image to a different one of equivalent functionality	Operations		X			Understand, Continue	Non-Persistence, Redundancy, Diversity	Software	Lower values are better. Changing a software image provides a moving target defense.

Metric Identifier	Summary Definition	Intended Use	Goal(s)				Objective(s)	Practice(s)	Layer(s)	Notes
			A	W	R	E				
METRIC-TECH-218	Percentage of deployed software for which updates are tracked using OVAL definitions	Operations	X				Understand	Analytic Monitoring, Substantiated Integrity	Software	Higher values are better.
METRIC-TECH-227	Length of time to redirect specific network packets to an alternate destination (i.e., not dictated by the destination addresses in the packets) in response to a detected threat or attack	Operations		X	X		Prevent, Continue	Adaptive Response, Deception	Cyber resource (network)	Lower values are better.
METRIC-TECH-228	Length of time to redirect all network packets to a pre-configured alternate destination (i.e., not dictated by the destination addresses in the packets)	Operations		X	X		Prevent, Continue	Adaptive Response, Unpredictability, Deception	Cyber resource (network)	Lower values are better. Redirection is in response to a detected threat or attack.
METRIC-TECH-230	Length of time to automatically redirect network packets to an alternate destination based on established/evolving packet redirection rules (i.e., not dictated by the destination addresses in the packets)	Operations		X	X		Prevent, Continue	Adaptive Response, Unpredictability, Deception	Cyber resource (network)	Lower values are better.
METRIC-TECH-238	Length of time for network packets selected by sensor module analytics to be redirected to a different destination (i.e., not the destination address in the packet) as a result of evolving packet redirection rules	Operations		X			Continue	Adaptive Response, Unpredictability	Cyber resource (network)	Lower values are better.

Metric Identifier	Summary Definition	Intended Use	Goal(s)				Objective(s)	Practice(s)	Layer(s)	Notes
			A	W	R	E				
METRIC-TECH-240	Number of packets intended to be redirected by a new rule that make it on to the internal network before the new rule is in force	Operations	X				Understand	Adaptive Response	Cyber resource (network)	Lower values are better.
METRIC-TECH-263	Length of time to reconstitute a database table from a backup data store	Operations			X		Reconstitute	Redundancy	Information store	Lower values are better.
METRIC-TECH-264	Length of time an attacker remains contained in a deception environment	Operations		X			Constrain	Segmentation	Cyber resource (system / network)	Higher values are better. This metric assumes (1) a controlled (deception) environment, (2) observation of when an attacker enters that environment, and (3) observation of when the attacker leaves that environment.
METRIC-TECH-265	Percentage of attackers in a deception environment who are unaware of their containment	Operations		X			Understand, Continue, Constrain	Analytic Monitoring, Deception, Segmentation	Cyber resource (system / network)	Higher values are better. This metric assumes (1) a controlled (deception) environment, (2) observation of when an attacker enters that environment, and (3) observation of attacker activities (e.g., exfiltration, installation of malware) in that environment.
METRIC-TECH-266	Percentage of times attacker goals can be discerned from activities in a deception environment	Operations		X			Understand, Continue, Constrain	Analytic Monitoring, Deception, Segmentation	Cyber resource (system / network)	Higher values are better. This metric assumes (1) a controlled (deception) environment, (2) observation of when an attacker enters that environment, and (3) observation of attacker activities (e.g., exfiltration, installation of malware) in that environment.
METRIC-TECH-267	Percentage of times an attacker in a deception environment closes out their encounter normally (i.e., removes traces of activity)	Operations		X			Understand, Continue, Constrain	Analytic Monitoring, Deception, Segmentation	Cyber resource (system / network)	Higher values are better. This metric assumes (1) a controlled (deception) environment, (2) observation of when an attacker enters that environment, (3) observation of when the attacker leaves that environment, and (4) observation of attacker activities upon leaving the environment.
METRIC-TECH-268	Length of time to determine what impact a cyber attack has had on a mission	Operations			X		Understand	Analytic Monitoring	Mission, Mission Process	Lower values are better. This metric assumes that (1) when a cyber attack began can be determined and (2) a way of determining or assessing mission impact has been established.

Metric Identifier	Summary Definition	Intended Use	Goal(s)				Objective(s)	Practice(s)	Layer(s)	Notes
			A	W	R	E				
METRIC-TECH-269	Length of time between when a defensive response is selected and when a mission capability is restored	Operations			X		Reconstitute	Adaptive Response	Mission, Mission Process	Lower values are better. This metric assumes that a definition of what it means for a mission capability to be restored has been established.
METRIC-TECH-270	Percentage of critical incident types for which pre-planned responses exist	Operations	X				Prepare	Coordinated Defense	Mission, Mission Process	Higher values are better. This metric assumes that a set of critical incident types have been defined.
METRIC-TECH-271	Length of time a mission is negatively affected after an attack	Operations		X			Continue	Adaptive Response	Mission, Mission Process	Lower values are better. This metric assumes that (1) a definition of what it means for a mission to be negatively affected has been established, (2) when a mission has been negatively affected can be determined, and (3) when a mission is no longer negatively affected can be determined.
METRIC-TECH-272	Length of time from opening of a trouble report to closing of the trouble report	Operations	X	X	X		Understand, Continue, Reconstitute	Adaptive Response	Mission, Mission Process	Lower values are better.

Bibliography

Allen, Julia, and Noopur Davis. "Measuring Operational Resilience Using the CERT® Resilience Management Model." September 2010. http://www.cert.org/archive/pdf/10tn030.pdf (accessed October 26, 2011).

Almeida, Raquel, Henrique Madeira, and Marco Vieira. "Benchmarking the Resilience of Self-Adaptive Systems: A New Research Challenge." *Proceedings of the 29th IEEE International Symposium on Reliable Distributed Systems.* 2010.

AMBER. "Final Research Roadmap." 31 December, 2009. http://www.amber-project.eu/documents/md_207_amber_d3-2.1_preliminaryresearchroadmap_v1.0.pdf (accessed May 26, 2011).

Bodeau, Deborah J., Richard D. Graubart, and Jennifer Fabius-Greene. *Cyber Security Governance, MTR100308, PR 10-3710.* Bedford, MA: The MITRE Corporation, 2010.

Bodeau, Deborah, and Richard Graubart. *Cyber Resiliency Engineering Framework, Version 1.0, MTR 110237 (Approved for Public Release, Case No. 11-4436).* Bedford, MA: The MITRE Corporation, 2011.

Boyer, Wayne, and Miles McQueen. "Ideal Based Cyber Security Technical Metrics for Control Systems." *Proceedings of the Second International Workshop on Critical Infrastructures Security.* Berlin: Springer-Verlag, 2008.

Brennan, J. J., et al. *Using Science and Technology Investment to Improve Department of Defense Cybersecurity Metrics.* Report for the Office of the Director of Defense Research & Engineering, 2009.

Brotby, W. Krag. *Information Security Management Metrics: A Definitive Guide to Effective Security Monitoring and Measurement.* Auerbach Publications, 2009.

Campbell, Philip. "Measures of Effectiveness: An Annotated Bibliography, SAND 2004-2902." *Sandia National Laboratories.* July 2004. http://prod.sandia.gov/techlib/access-control.cgi/2004/042902.pdf (accessed October 26, 2011).

Chairman of the Joint Chiefs of Staff. "Information Assurance (IA) and Support to Computer Network Defense (CND), CJCSI 6510.01F." February 9, 2011. http://www.dtic.mil/cjcs_directives/cdata/unlimit/6510_01.pdf (accessed October 26, 2011).

CIS. "The CIS Security Metrics v.1.1.0." *The Center for Internet Security.* November 1, 2010. https://benchmarks.cisecurity.org/tools2/metrics/CIS_Security_Metrics_v1.1.0.pdf (accessed October 26, 2011).

ENISA. "Measurement Frameworks and Metrics for Resilient Networks and Services: Technical report (Discussion draft)." February 21, 2011. http://www.enisa.europa.eu/act/res/other-areas/metrics/reports/metrics-tech-report/at_download/fullReport (accessed October 26, 2011).

Foote, Scott, Mark Kramer, and Beth Yost. "Alternative Processes and Operations Controlled via a Cyber Operations Center (CyOC), PR # 11-1567." *The MITRE Corporation.* 2011. http://www.mitre.org/work/areas/research/2011iebriefings/05MSR160-JO.pdf (accessed September 13, 2011).

Gawande, Atul. *Better: A Surgeon's Notes on Performance .* New York, NY: Metropolitan Books, 2007.

Goldman, Harriet. "Building Secure, Resilient Architectures for Mission Assurance (presentation, PR # 10-3728)." *Presentations at the 3rd Workshop on Cyberspace Research (CSW'10).* November 15, 2010. http://csc.latech.edu/crw10/slides/Goldman.ppt (accessed September 15, 2011).

Herrmann, Debra S. *Complete Guide to Security and Privacy Metrics: Measuring Regulatory Compliance, Operational Resilience, and ROI.* Auerbach Publications, 2007.

IATAC. "Measuring Cyber Security and Information Assurance: State-of-the-Art Report (SOAR)." May 9, 2009. http://iac.dtic.mil/iatac/download/cybersecurity.pdf (accessed October 26, 2011).

INCOSE. "Systems Engineering Measurement Primer." March 1998. http://www.afit.edu/cse/docs/guidance/System%20Engineering%20Measurement%20Primer%201998-03.pdf (accessed October 26, 2011).

Jansen, Wayne. "Directions in Security Metrics Research, NISTIR 7564." March 2009. http://csrc.nist.gov/publications/nistir/ir7564/nistir-7564_metrics-research.pdf (accessed September 26, 2011).

NIST. "NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View." March 2011. http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf (accessed October 26, 2011).

—. "Performance Measurement Guide for Information Security, NIST SP 800-55 Revision 1." July 2008. http://csrc.nist.gov/publications/nistpubs/800-55-Rev1/SP800-55-rev1.pdf (accessed October 26, 2011).

Risk Steering Committee. "DHS Risk Lexicon, 2010 Edition." September 2010. http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf (accessed October 26, 2011).

Yan, Zhenyu, and Yakov Haimes. "Risk-based Multiobjective Resource Allocation with Multiple Decisionmakers in Risk Management of Large-scale Hierarchical Systems, part I: Theory and Methodology." *Systems Engineering, 14(1), 2011: 1-16.* February 2, 2010. http://www3.interscience.wiley.com/cgi-bin/fulltext/123270626/PDFSTART (accessed September 21, 2011).