MTR180314
MITRE TECHNICAL REPORT

MITRE

Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring

Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods

Deborah J. Bodeau
Richard D. Graubart
Rosalie M. McQuaid
John Woodill

September 2018

Dept. No.: T8A2
Project No.: 5118MC18-KA

Bedford, MA

Abstract

This report is intended to serve as a general reference for systems engineers, program management staff, and others concerned with assessing or scoring cyber resiliency for systems and missions; selecting cyber resiliency metrics to support cyber resiliency assessment; and defining, evaluating, and using cyber resiliency measures of effectiveness (MOEs) for alternative cyber resiliency solutions. Background material is provided on how cyber resiliency scores, metrics, and MOEs can be characterized and derived; based on that material, a wide range of potential cyber resiliency metrics are identified. Topics to address when specifying a cyber resiliency metric are identified so that evaluation can be repeatable and reproducible, and so that the metric can be properly interpreted. A tailorable, extensible cyber resiliency scoring methodology is defined. A notional example is provided of how scoring, metrics, and MOEs can be used by systems engineers and program management to identify potential areas of cyber resiliency improvement and to evaluate the potential benefits of alternative solutions.

This page intentionally left blank.

Executive Summary

Introduction. This report is intended to serve as a general reference for systems engineers, program management staff, and others concerned with cyber resiliency metrics for systems and missions. Such stakeholders may be interested in

- Assessing or scoring cyber resiliency to compare a current or planned system with an ideal;
- Selecting cyber resiliency metrics which can be evaluated in a lab, test, or operational setting to support cyber resiliency assessment; and/or
- Defining, evaluating, and using measures of effectiveness (MOEs) for alternative cyber resiliency solutions.

Cyber resiliency metrics can inform investment and design decisions. They are closely related to, but not identical with, metrics for system resilience and security, and share challenges related to definition and evaluation with such metrics. A cyber resiliency metric is derived from or relatable to some element of the Cyber Resiliency Engineering Framework (CREF)[1] – a cyber resiliency goal, objective, design principle, technique, or implementation approach to a technique. As illustrated in Figure ES-1, the selection and prioritization of elements of the CREF for a given system or program is driven by the risk management strategy of the program or the system's owning organization.

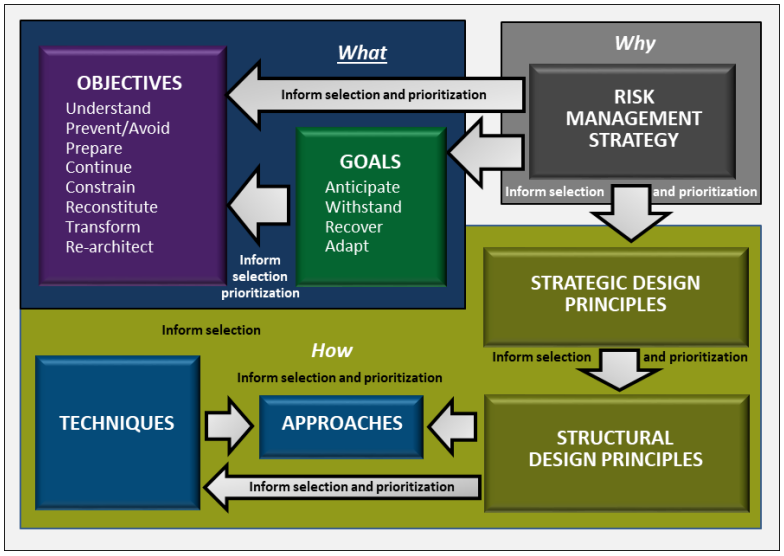

Figure ES-1. Cyber Resiliency Engineering Framework: Mapping the Cyber Resiliency Domain[2]

By contrast, MOEs for alternative cyber resiliency solutions – i.e., combinations of architectural decisions, technologies, and operational processes intended to improve how well cyber resiliency goals and objectives are achieved by applying cyber resiliency design principles and techniques – may not be cyber resiliency metrics *per se*. Cyber resiliency MOEs can take the form of changes in mission MOEs or measures of performance (MOPs), metrics related to adversary activities, or other risk factors.

A scoring methodology for cyber resiliency can be used to assess how well a given system can meet its operational or mission objectives, and to compare alternative solutions. Any scoring methodology is inherently situated in a programmatic, operational, and threat context; for cyber resiliency scoring, the

[1] The CREF provides a structure for understanding different aspects of cyber resiliency and how those aspects interrelate.
[2] Adapted from Figure 1 of the Initial Public Draft (IPD) of NIST SP 800-160 Vol. 2 [1].

threat model is particularly important. The Situated Scoring Methodology for Cyber Resiliency (SSM-CR) provides a way to capture stakeholder priorities, restating what cyber resiliency objectives and more detailed CREF elements (sub-objectives and activities) mean for a given system or program, and to capture subject matter expert (SME) assessments of how well the relevant activities are or can be performed.

Supporting evidence for qualitative assessments can be developed by identifying and evaluating relevant cyber resiliency metrics and MOEs for alternative solutions; in addition, a set of cyber resiliency metrics can be selected and tailored for inclusion in a larger metrics program. Such metrics can be defined using a template to ensure repeatability and reproducibility. A catalog of representative cyber resiliency metrics has been developed and is described in a companion report.

The remainder of this Executive Summary expands upon these points. The report itself provides considerable detail, and is designed to be a general reference on cyber resiliency metrics.

Why consider cyber resiliency metrics? Cyber resiliency – *the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources* – is increasingly a concern for mission owners, program managers, and systems engineers. When these stakeholders consider a system (or a system-of-systems, as identified with a mission or a mission thread, or a family of systems, as identified with an acquisition program) from the standpoint of cyber resiliency, they tend to pose several questions:

- Which aspects of cyber resiliency matter to us? As illustrated in Figure ES-2, aspects of cyber resiliency which can be prioritized and assessed include properties, capabilities, and behaviors.
- How well does the system provide these aspects? That is,
    - How completely or with how much confidence are *properties* and *capabilities* provided?
    - How quickly, completely, and confidently can *behaviors* occur?
- What risks – to the missions the system supports, to the program, or to the information the system handles and to stakeholders in the security of that information – are addressed by the way the system provides cyber resiliency? What risks remain?

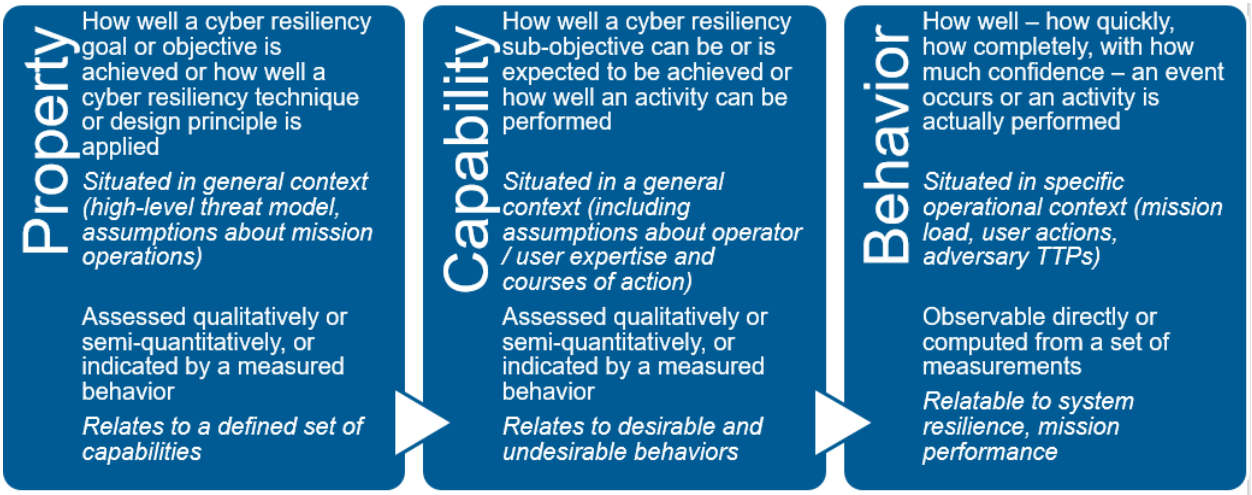

Figure ES-2. Assessable or Measurable Aspects of Cyber Resiliency for a System

If the system is not sufficiently cyber resilient to address stakeholder concerns, a set of alternative cyber resiliency solutions can be defined, by applying cyber resiliency design principles to make architectural

decisions, and by using cyber resiliency techniques, approaches to implementing those techniques, and specific technologies, products, and processes or procedures. Two questions then arise:

- How much cyber resiliency improvement (or risk reduction) does each alternative solution provide?
- Is any combination of solutions sufficient to address stakeholder concerns?

Cyber resiliency metrics – measurements, values computed from measurements and other parameters, scores, and qualitative or semi-quantitative assessments – are used to answer these questions. Different forms of metrics are associated with different aspects of cyber resiliency and with different analytic processes and decisions to be supported. Measurements and quantitative values computed from measurements support detailed analysis of system behaviors and thus of the implications of alternative solutions for mission MOEs and MOPs. Scores, qualitative assessments, and semi-quantitative assessments encode stakeholder priorities and subject matter expert (SME) judgments to support comparison of alternatives. However, the line between different forms of metrics is not well-defined: quantitative metrics such as "time to recover" or "percentage of mission functionality preserved" can incorporate SME judgments and can support scores and qualitative assessments.

Related metrics. The cyber resiliency problem domain overlaps with the problem domains of system resilience and security. Many metrics from those domains can be repurposed or refined to support cyber resiliency analysis. Security metrics generally focus on security practices and security capabilities (i.e., capabilities supporting the security objectives of confidentiality, integrity, availability, and accountability), or on metrics related to asset loss, rather than on mission assurance.

As illustrated in Figure ES-3, system resilience metrics are generally founded on a temporal model of disruption and recovery which assumes the feasibility of timely detection and response; detection and recovery are more challenging when attacks are orchestrated by advanced cyber adversaries.

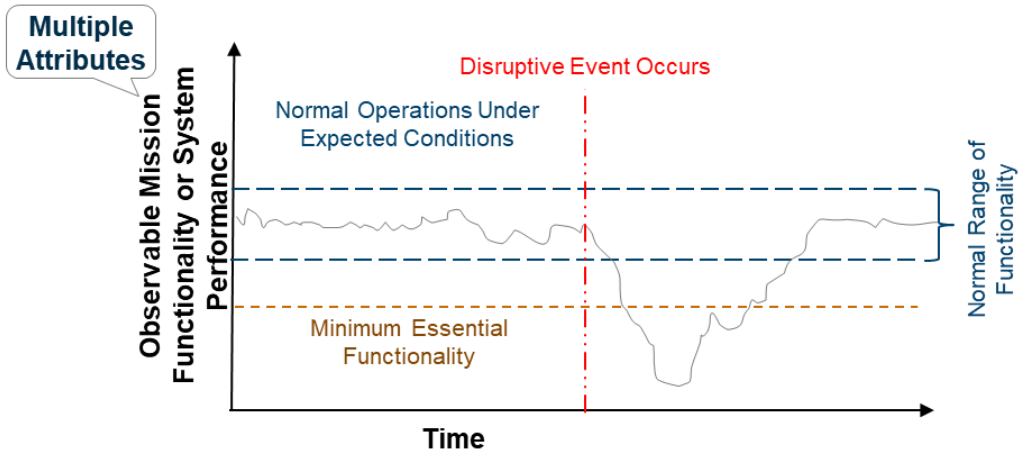

Figure ES-3. System Resilience Metrics Are Based on Time and Level of Performance

As illustrated in Figure ES-4, cyber resiliency explicitly considers attacks on and compromises of cyber resources. These may fail to be detected for some time, while a cyber adversary performs activities at different stages of a cyber attack lifecycle prior to taking an obviously disruptive action. (And if the attack is focused on exfiltration, adversary-caused disruption may not occur.) Thus, performance metrics are necessary but not sufficient to understand a system's cyber resiliency; metrics are needed for properties and capabilities as well.

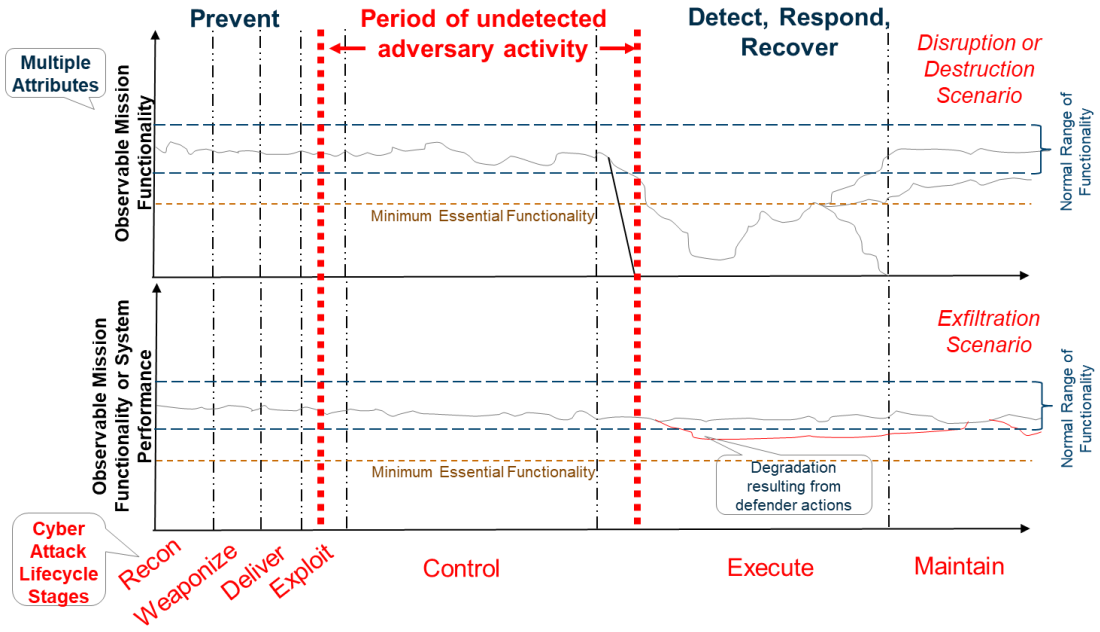

Figure ES-4. Many Activities in the Cyber Attack Lifecycle Can Go Undetected

System resilience and security metrics are closely related to risk metrics. Cyber resiliency metrics related to a risk measure (or assess the extent of) conditions predisposing toward greater adverse consequences, propagation of consequences, consequence reduction, and effects of alternatives on potential adversary actions. Unlike risk-related system resilience and security metrics, cyber resiliency metrics generally do not include metrics related to vulnerability severity, although changes in event likelihood or vulnerability severity can constitute MOEs for cyber resiliency solutions. The relationship between cyber resiliency metrics and related metrics is summarized in Figure ES-5; while cyber resiliency metrics can repurpose security, risk, or resilience metrics, the specification of those metrics must be tailored to reflect the assumptions underlying cyber resiliency engineering, systems engineering, and mission and cyber operations.

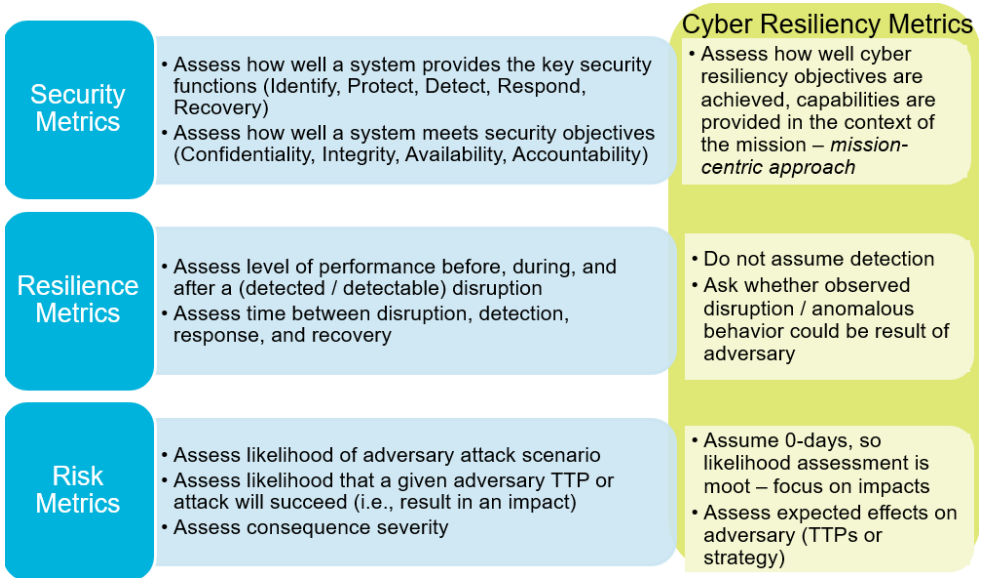

Figure ES-5. Cyber Resiliency Metrics Can Repurpose Security, Risk, or Resilience Metrics

Challenges. Cyber resiliency metrics share definitional and evaluative challenges with metrics for related emergent properties, particularly security and system resilience. These challenges relate to

- Complexity and emergent properties. Emergence refers to the inability to determine system-level properties solely from the properties of individual components. System complexity makes the definition of metrics for emergent properties, and for corresponding capabilities and behaviors, more difficult. Analysis and supporting metrics need to account for behaviors typical of complex systems such as compounding, cascading, and feedback.
- Contextuality. Cyber resiliency, like mission assurance, is meaningful in the context of the mission (or set of missions); the operational and supporting processes for using, maintaining, administering, and protecting mission systems; and the threat environment. Cyber resiliency metrics are therefore defined and evaluated in a context which may be broadly or specifically described.
- Feasibility of evaluation. For the use of a metric to be feasible, it must be well specified so that it can evaluated in a reproducible, repeatable way. The evaluation of any specific metric has an associated cost, to gather, process, and store the information used to produce the value. The data (or inputs from subject matter experts) must be available, and the evaluation of the metric from those inputs must be made, at a cost which is acceptable to the stakeholders whose questions the metric is intended to answer and in a timeframe consistent with the decisions the metric is intended to support.

One consequence of these challenges is that any single figure-of-merit for cyber resiliency computed from measurements will be strongly situated in an assumed context or will attempt to represent a wide range of contexts. A strongly situated metric must be properly presented to avoid being misinterpreted as general. Evaluation of a metric which seeks to represent a wide range of contexts may be infeasible, except when evaluation involves modeling and simulation (M&S), which perforce encodes assumptions about the system and its operational and threat environments. Thus, any complicated formula for computing a single figure-of-merit from measurements is best treated as a starting point for discussion: an artifact which different stakeholders can look at together and use to discuss their different perspectives on what cyber resiliency means to them.

What makes a metric a cyber resiliency metric? The relationship between any given metric and cyber resiliency can be articulated using the CREF. The CREF defines the "what" of cyber resiliency in terms of goals (Anticipate, Withstand, Recover, and Adapt, consistent with resilience engineering) and objectives (Prevent / Avoid, Prepare, Continue, Constrain, Reconstitute, Transform, Re-Architect, and Understand). The cyber resiliency goals characterize high-level system properties (awareness, robustness, recoverability, and adaptability). The cyber resiliency objectives describe more specific properties (hardness, readiness, continuity, damage limitation, reconstitution, operational agility, technical agility, and accountability). These properties can be used to drive the definition of metrics by defining representative sub-objectives or capabilities and the activities or behaviors which collectively achieve those sub-objectives. Many metrics related to time, performance, and extent of coverage have been derived from the objectives / properties → sub-objectives → activities part of the CREF.

The CREF also defines the "how" of cyber resiliency in two ways. First, cyber resiliency design principles distill engineering decisions and design patterns. Second, cyber resiliency techniques refer to sets or classes of technologies and processes intended to achieve one or more goals or objectives by providing types of capabilities. To support more detailed engineering analysis, multiple representative approaches to implementing each technique are identified. An approach is a subset of the technologies and processes included in a technique, defined by how the capabilities are implemented or how the intended outcomes are achieved. Metrics related to design principles or techniques generally capture how extensively these CREF constructs have been applied – to what percentage of cyber resources, at how many architectural layers, at how many locations in the system architecture.

For any given system or program, the cyber resiliency objectives, sub-objectives, and activities must be tailored or interpreted to be meaningful in the context of the system's missions or business functions and its operational environment. The metrics associated with those activities must therefore be tailored to be meaningful for the system. Similarly, metrics associated with cyber resiliency design principles, techniques, and approaches must be tailored to reflect the system's technical environment – its architecture and constituent technologies.

Many of the metrics defined from the CREF can be also be viewed from a mission assurance perspective (e.g., relatable to mission MOPs). Alternately, an MOE for a cyber resiliency solution can take the form of a change in a mission MOE or MOP – that is, the cyber resiliency solution MOE may not be a cyber resiliency metric per se. Similarly, many of the metrics defined from the CREF can also be viewed from a risk management perspective, e.g., relatable to effects on adversary tactics, techniques, and procedures (TTPs). Alternately, an MOE for a cyber resiliency solution can take the form of a change in one or more risk factors (e.g., likelihood of adverse consequences, extent to which an adversary is deterred).

Cyber resiliency scoring. Scoring, ranking, and rating systems provide semi-quantitative values to enable comparison against a theoretical ideal or among different alternatives. This report describes a proposed system for cyber resiliency and describes issues which must be addressed to ensure that such systems are applied properly.

The Situated Scoring Methodology for Cyber Resiliency (SSM-CR) is a tailorable scoring methodology intended to provide Program Managers with a simple relative measure of how cyber resilient a given system is, and of whether and how much different alternatives change that measure. SSM-CR is situated or context-adjusted in two ways: First, it reflects stakeholder priorities (i.e., which objectives, sub-objectives, and capabilities are important). Second, performance assessments (i.e., how well prioritized capabilities are provided or how well prioritized activities are actually performed) are made with respect to stated assumptions about the operational and threat environments. An underlying threat model is an essential input to a cyber resiliency assessment.

SSM-CR produces a top-level score, individual scores for those objectives which are determined to be relevant, and lower-level assessments of activities or capabilities. Differences in cyber resiliency scores for alternative solutions are traceable to differences in the performance assessments for specific activities. By identifying the activities or capabilities which a solution is expected to improve, systems engineers can identify corresponding metrics for which values are expected to improve; changes in those metrics constitute MOEs for the solution.

Defining a cyber resiliency metrics program. For any given system, mission, or organization, a large number of possible cyber resiliency metrics can be identified. However, metric evaluation involves time and effort, and may involve investment in specialized tools to gather the necessary data. Therefore, when selecting cyber resiliency metrics for possible inclusion in a metrics program, several considerations are important. These considerations include the class of decisions the metrics are intended to support (e.g., engineering vs. investment or programmatic vs. tactical operations), the measurement domain (e.g., physical, information / technical, cognitive, or social / organizational), the type of system to be measured, and the aspects of cyber resiliency (e.g., objectives, techniques) to be assessed. The attributes of these considerations may be prioritized, with the relative priorities informing the selection of potential metrics.

The definition of a cyber resiliency metrics program involves selecting metrics; tailoring them to reflect organization- or system-specific assumptions, priorities, and constraints; specifying them so that evaluation can be repeatable and reproducible; and evaluating them so that their values can be tracked over time or in response to changes in the environment or underlying assumptions. A metric specification can be captured by using a template, as included in this report. In addition to supporting evaluation, metric specification reduces the potential for misinterpretation or misrepresentation of what metric values mean.

Table of Contents

List of Figures

List of Tables

1 Introduction

Cyber resiliency – *the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources* [1] – is increasingly an explicit concern at varying scopes or scales, ranging from components to critical infrastructure sectors, regions, and nations. Cyber resiliency for systems, missions, and programs is one aspect of trustworthiness to be addressed by systems security engineering [2]. In order to provide trustworthy systems, systems engineers and architects seek ways to apply cyber resiliency concepts and to integrate resilience-enhancing technologies into architectures, designs, and operational systems [3] [4] [5] [6]. As they do so, they need to evaluate the relative effectiveness of architectural alternatives, as well as new technologies, products, or processes, for improving cyber resiliency and mission assurance. Cyber resiliency metrics create evidence that can be used in an assurance case, as described in NIST SP 800-160 Vol. 1 [2]. Similarly, program managers seek to determine whether investments in cyber resiliency will enable them to meet mission and security requirements more efficiently. This report is intended to serve as a general reference for systems engineers, program management staff, and others concerned with cyber resiliency metrics for systems and missions.

A wide variety of cyber resiliency metrics have been proposed [7]. Examples include time between beginning of a disruption and complete recovery; minimum level of system performance during a disruption; qualitative assessment of how well a system meets a cyber resiliency objective[3]; and percentage of attack types a system can detect. Cyber resiliency metrics vary widely in form (e.g., qualitative, quantitative, semi-quantitative), fidelity (rigor and granularity), and generality (e.g., applicable to any system, specific to Windows environments, unique to a single class of cyber-physical systems). This variety is due to multiple sources, including

- The nature of the decisions a metric is intended to support (e.g., engineering, programmatic, or operational);
- The type of cyber resiliency construct (e.g., goal, objective, design principle, technique, solution) for which a metric is intended to answer (or support an answer to) a question;
- Whether a metric is intended to measure system properties, system behavior, or the relative effectiveness of a cyber resiliency solution;
- The assumptions about the system environment – particularly the mission and the threats against the mission and/or cyber resources – in which a metric is intended to be meaningful; and
- The evaluation environment, which reflects the overall approach to measuring or assessing cyber resiliency. As discussed in [8] [9], assessment can be metric-based, relying on data gathered in an operational or laboratory environment or on subject matter expert (SME) judgment, or model-based, relying on such methods as modeling and simulation (M&S) or model-based systems engineering (MBSE).

This paper presents a concept for using scoring and metrics to compare and evaluate the effectiveness of potential cyber resiliency solutions to the problems faced by systems and programs, in the context of a stated threat, operational, and programmatic environment. To do so, this paper provides a framework for characterizing and defining cyber resiliency metrics and measures of effectiveness (MOEs), building on and extending prior work [7]. It updates and extends the 2012 cyber resiliency metric template [10]. This paper also defines a tailorable, situated scoring system for cyber resiliency, to support engineering analysis and programmatic decisions. Companion papers present the Cyber Resiliency Metrics Catalog

[3] Section 2 describes cyber resiliency constructs from the Cyber Resiliency Engineering Framework (e.g., goals, objectives, techniques, design principles) only in enough detail to inform the discussion of metrics. For more detail, see [4] [3].

[11] and the Vehicle Use Case [12] in detail. This paper focuses on metrics-based assessment approaches. However, many metrics defined for evaluation in an operational environment can also be represented and evaluated in a model-based setting.

1.1 Concept of Use for Cyber Resiliency Scoring and Metrics

Cyber resiliency scoring methods and metrics are tailorable resources to aid systems engineers, program managers, and others supporting risk management for systems or programs in which cyber resiliency is a concern. A scoring system and a set of metrics are only meaningful in the context of programmatic and engineering decisions, under risk framing assumptions (in particular, assumptions about cyber threats, as well as assumptions about operating conditions). Scores and metrics are produced in the course of analysis activities, guide subsequent analysis activities, and support decisions regarding the need for and selection of alternative solutions.

Figure 1 illustrates the overall concept of use for the cyber resiliency scoring methodology and metrics catalog described in this paper. (This description uses the Cyber Resiliency Engineering Framework (CREF), which is described in more detail in Section 2.) Systems engineering tasks in which the scoring methodology is used are outlined in red; those which use the catalog are outlined in green. The scoring methodology is used in the first two steps, as the relative priorities of cyber resiliency objectives, sub-objectives, and capabilities are assessed and used to restrict the solution space. The scoring methodology is also used in the third step, as a bridge to the catalog. The extent to which key capabilities are provided are assessed, and metrics related to those capabilities are identified from the catalog for potential use as MOEs. Those metrics, as well as metrics related to the mission and potential effects on adversary activities, are tailored and documented, using the cyber resiliency metrics template, and may be added to the catalog. In the final step, MOEs for selected alternatives are evaluated; the results of this evaluation are reflected in the performance assessments for the capabilities the alternatives improve and in the overall cyber resiliency score.

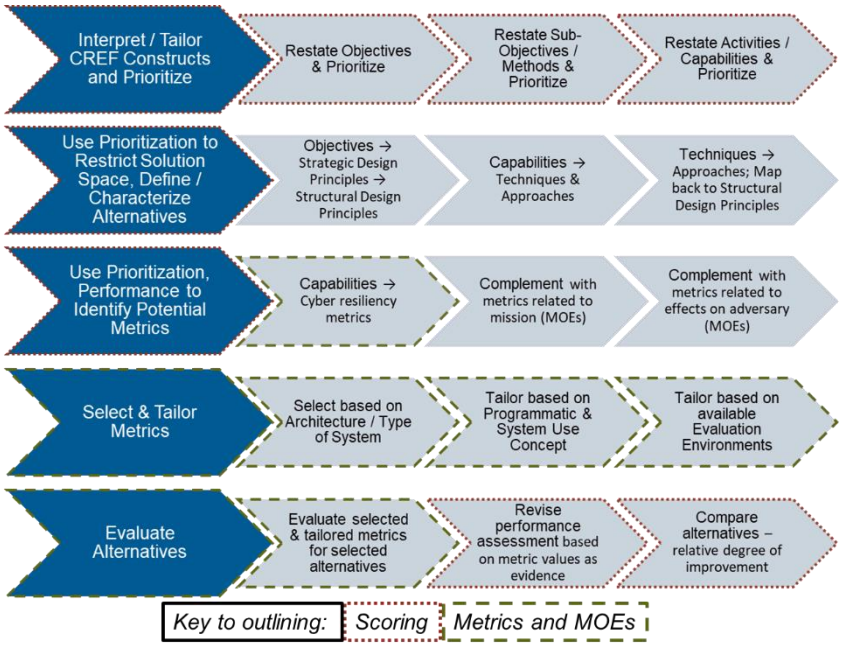

Figure 1. Concept of Use for Cyber Resiliency Scoring and Metrics Catalog

Figure 2 indicates how this concept fits into the Structured Cyber Resiliency Analysis Methodology (SCRAM, [13]). Tailoring and prioritizing objectives, sub-objectives, and capabilities (1) in the context of a defined threat model, system concept, and programmatic strategy (2) are an outcome of the first step in

SCRAM, *Understand the mission and threat context*. The second step includes identifying how cyber resiliency is already being applied and any cybersecurity issues. Identifying these can indicate existing metrics which could be repurposed for cyber resiliency (3). The results of the identification are used in the initial baseline assessment (4) or scoring, the final task in the second step of SCRAM. In the third step, potential applications of cyber resiliency design principles, techniques, and implementation approaches are identified; metrics associated with these can be identified (5) from the metrics catalog. Alternatives are identified in the fourth step, enabling the metrics from the catalog and the metrics identified earlier (3) to be specified in enough detail that they can be evaluated to support comparisons (6). MOEs and metrics, and scores which are informed by these, are evaluated at the end of the fourth step and revisited at the start of the fifth and final step of SCRAM (7).

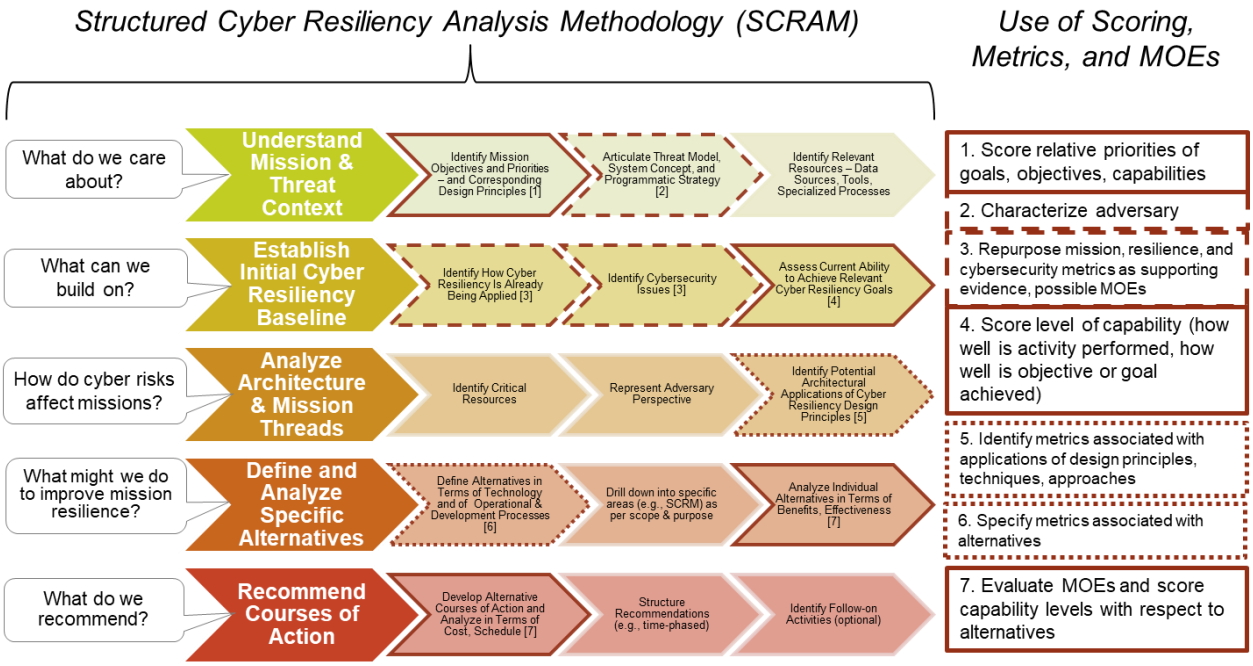

Figure 2. Cyber Resiliency Scoring and Metrics Catalog in SCRAM

1.2 Cyber Resiliency and Other Problem Domains

The problem domain for cyber resiliency overlaps with the problem domains for security and resilience engineering, particularly when focused on systems, systems-of-systems identified with or supporting missions, and programs. Cyber resiliency differs from security in its focus on the mission, emphasizing the need to minimize mission impacts rather than the need to minimize losses of information, information systems, or other assets. Cyber resiliency differs from resilience against non-adversarial forms of adversity in that analysis of any potential disruption involves asking, *What if this disruption was caused by an adversary – what would that imply for the expected effectiveness of response and recovery efforts? Whatever caused this disruption, how could cyber adversaries take advantage of the direct and indirect results of the disruption to achieve their goals?* The overlap between the problem domains of cyber resiliency, security, and resilience means that many metrics defined for the security or resilience domain may be relevant to, or tailorable for, cyber resiliency.

1.3 Overview of This Document

This is a large document, intended to serve as a general reference. Each section provides discussion of key topics, with details placed in an Appendix. While this document can be read end-to-end, a more

fruitful approach is for readers to identify the sections of greatest interest to them from the following description, and to consult other sections as necessary for amplification of related topics.

Section 2 presents background on metrics and their uses, including key concepts and terminology; challenges for the definition, evaluation, and use of metrics; and ways to characterize cyber resiliency metrics. For more information on cyber resiliency and on the Cyber Resiliency Engineering Framework (CREF), see [1]. Appendix A provides more detail, describing how cyber resiliency constructs – goals, objectives, sub-objectives, activities, and design principles – relate to metrics and MOEs.

Section 3 describes how a representative set of metrics (Appendix B) was developed from the CREF. Material in Appendix B has been used to update and extend the 2012 catalog [10]; that extended catalog is briefly described in Section 2.6 and is presented in a companion report [11].

Engineering and programmatic decisions can be supported by individual metrics such as "how quickly mission-critical data store ABC can be reconstituted from a protected backup or gold copy" or "percentage of mission-critical data stores that have been validated as uncorrupted since the initiation of a responsive cyber course of action." The selection of metrics for evaluation is driven by a variety of factors. To ensure that evaluation can be reproducible and repeatable, a metric must be well-defined. Section 4 describes selection criteria and identifies topics which should be covered in a metric definition; a tailorable template is provided in Appendix C.

Two of the factors guiding the selection of individual metrics for evaluation are (1) stakeholder objectives and concerns and (2) engineering judgment regarding which aspects of system performance merit improvement. A scoring system provides a useful way to capture information about stakeholder priorities and subject matter expert (SME) judgment on performance. Section 5 discusses the challenges of scoring systems for cybersecurity and cyber resiliency. The Situated Scoring System for Cyber Resiliency (SSM-CR), an example of a tailorable scoring system, is described in detail in Appendix D.

2 Background

This section provides presents key concepts and terminology; provides a brief overview of the Cyber Resiliency Engineering Framework; identifies challenges for the definition, evaluation, and use of metrics; and provides background on how cyber resiliency metrics can be characterized.

2.1 Key Concepts and Terminology

Cyber resiliency is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources. This ability can be the property of a component, sub-system, system, platform, system-of-systems, mission, organization, critical infrastructure sub-sector or sector, or nation. This report does not consider scopes beyond the organization, and focuses on cyber resiliency metrics for missions, systems-of-systems which can be identified with the missions they support, systems, and sub-systems. The focus is on metrics which support engineering decisions.

A *measure of effectiveness* (MOE) is "an indicator used to measure a current system state, with change indicated by comparing multiple observations over time." [14] For DoD acquisitions, a MOE is "the data used to measure the military effect (mission accomplishment) that comes from using the system in its expected environment. That environment includes the system under test and all interrelated systems, that is, the planned or expected environment in terms of weapons, sensors, command and control, and platforms, as appropriate, needed to accomplish an end-to-end mission in combat." [15]

Metrics are the result of a process or method for measuring, evaluating, or comparing similar objects. Metrics can take a variety of *forms* (including quantitative, qualitative, semi-quantitative, and nominal); *types* (including measurements; evidence or observables; metrics computed or derived from measurements or evidence; and expert judgments); and relationships to intended effects (ranging from direct representations to indirect indications). Within a system, measurements and evidence are *evaluated* or *obtained* at a location (e.g., an architectural layer; a point that can be designated in an architectural diagram); computed or derived metrics are based on measurements and/or evidence which can come from one or more locations. Metrics for cyber resiliency are an active area of discussion and investigation [7]. A cyber resiliency metric becomes a measure of effectiveness when it is used to evaluate the relative effectiveness of a cyber resiliency solution relative to a specific mission.

Evaluation of cyber resilience metrics – like any metric evaluation – involves representations of or assumptions about characteristics of the environment in which resilience is sought [16]. *Evaluation environments* can range from the highly situated and specific (e.g., a specific system in an operational context), to representative of a specific set of characteristics with others left unspecified (e.g., a cyber range, a modeling and simulation (M&S) environment), to conceptually representative (e.g., a tabletop exercise; an expert evaluation). Defining the system (and its boundaries) can be particularly challenging [17]; in a contested cyber environment, the system must be viewed as a socio-technical system which includes cyber defenders, mission users, and adversaries.

A cyber resiliency *solution* is a technology, practice, or set of technologies and practices, integrated into a system to improve its cyber resiliency. It thereby provides a solution to a problem of the form "how can cyber resiliency be improved?" or "how can the system be made more resilient against cyber attack (or in a cyber-contested environment)?" That problem includes an assumed *context*, which includes a threat model, an operational environment, and a technical environment. The assumed operational environment identifies the concept of operations (CONOPS) for the system and can include the missions the system supports as well as the threats against those missions, the organization(s) responsible for the missions, the system, and the information it handles. The technical environment includes, at a minimum, the type of system for which the problem is posed, e.g., CPS, enterprise information technology (EIT), weapon system (WS). Depending on how completely the context is described, a cyber resiliency solution can be

quite general (e.g., a design pattern for non-persistent services in an enterprise) or very specific (e.g., a combination of configuration settings for specific products in an as-deployed CPS).

In its assumed context, a system already has some *baseline* cyber resiliency. Measuring improvements to that baseline requires that its cyber resiliency properties be measured, and then that changes resulting from the solution be measured.

The concept of a *cyber course of action* (CCoA) is central to applying cyber resiliency in an operational setting. A CCoA is a set of activities or tactics, techniques, and procedures (TTPs) employed by automation, cyber defenders (e.g., staff in a Security Operations Center (SOC) or a Cyber Security Operations Center) and, as needed, other cyber staff (e.g., staff in a Cyber Operations Center, system administrators, network operators) and mission staff or end users in response to threat events or other circumstances (e.g., indications and warnings (I&W), contingencies). [4] CCoAs can be defined solely for adversarial threats, in which case the documentation of CCoAs takes the form of a "cyber playbook." CCoAs defined for a broader set of threat types (e.g., power failure, human error, natural disaster) are typically documented in a contingency or continuity of operations (COOP) plan. Some predefined CCoAs, particularly those which respond to faults and failures, can be automated. The definition and execution of a CCoA is predicated on knowledge or assumptions about dependencies and interactions among cyber resources, and particularly about dependencies and interactions among resources involved in administration, security policy enforcement, and active defense.

A CCoA is intended to mitigate the mission effects of adversity. In addition, a CCoA is intended to have one or more effects on threat events. A vocabulary of six high-level effects (redirect, preclude, impede, detect, limit, and expose) and fourteen lower-level effects (deter, divert, and deceive; prevent and preempt; degrade and delay; detect; contain, shorten, recover, and expunge; and scrutinize and reveal) can be used to describe the intended effects of a CCoA, a defensive TTP, or a cyber resiliency solution on a threat event [18]. Some of these possible desired effects are specific to adversarial events: redirect and, at a lower level, deter, divert, and deceive. The remaining desired effects are relevant to non-adversarial as well as adversarial threat events.

Other terms used in the descriptions of capabilities, activities, or metrics are defined in the Glossary (Appendix E), and include[4] asset, attack surface, component, cyber asset, cyber resource, data asset (or information asset), dynamic, mission / business function, mission-critical, mission-supporting, resource, security-critical, and TTPs.

2.2 Cyber Resiliency Engineering Framework

The Cyber Resiliency Engineering Framework provides a structured way to understand the cyber resiliency domain – the problem space and the solution space. As illustrated in Figure 3, the CREF includes two primary constructs to describe the desired properties of a system (the "what" of cyber resiliency): cyber resiliency goals[5] and objectives[6]. These objectives can be further refined into sub-objectives and representative activities or capabilities by which those sub-objectives are achieved.

---

[4] These definitions are taken from [4], with the exception of the definition of attack surface (taken from [3]).

[5] The cyber resiliency goals in the CREF are those in the Initial Public Draft of NIST SP 800-160 Vol. 2 [1]. As noted in Section 2.1.1 of [1], many different definitions have been offered for resilience. In these definitions, alternatives to anticipate include plan, prepare for, and resist, while alternatives to withstand include absorb and survive.

[6] System properties are typically described using nouns, e.g., security, safety, cyber resiliency. (See [155] for an approach to measuring security as a system property.) The CREF uses verbs to identify goals and objectives: While, in many cases, a corresponding noun could be given, the common uses of those nouns typically do not include a connotation of considering activities by advanced cyber adversaries. "How well" a given cyber resiliency goal or objective is achieved is a cyber resiliency property.

The CREF also includes two constructs to describe the solution space (the "how" of cyber resiliency): cyber resiliency design principles and cyber resiliency techniques[7]. As Figure 3 indicates, these two "how" constructs have further elaboration. Cyber resiliency design principles can be either strategic or structural. A number of representative implementation approaches have been defined for cyber resiliency techniques. The set of approaches is not intended to be exhaustive; which approaches are relevant depends on the type of system (e.g., enterprise information technology (EIT), CPS, weapon system) as well as on other factors such as the technical architecture, governance, and maturity (in the context of the program's technical risk management strategy, e.g., whether emerging technologies can be applied).

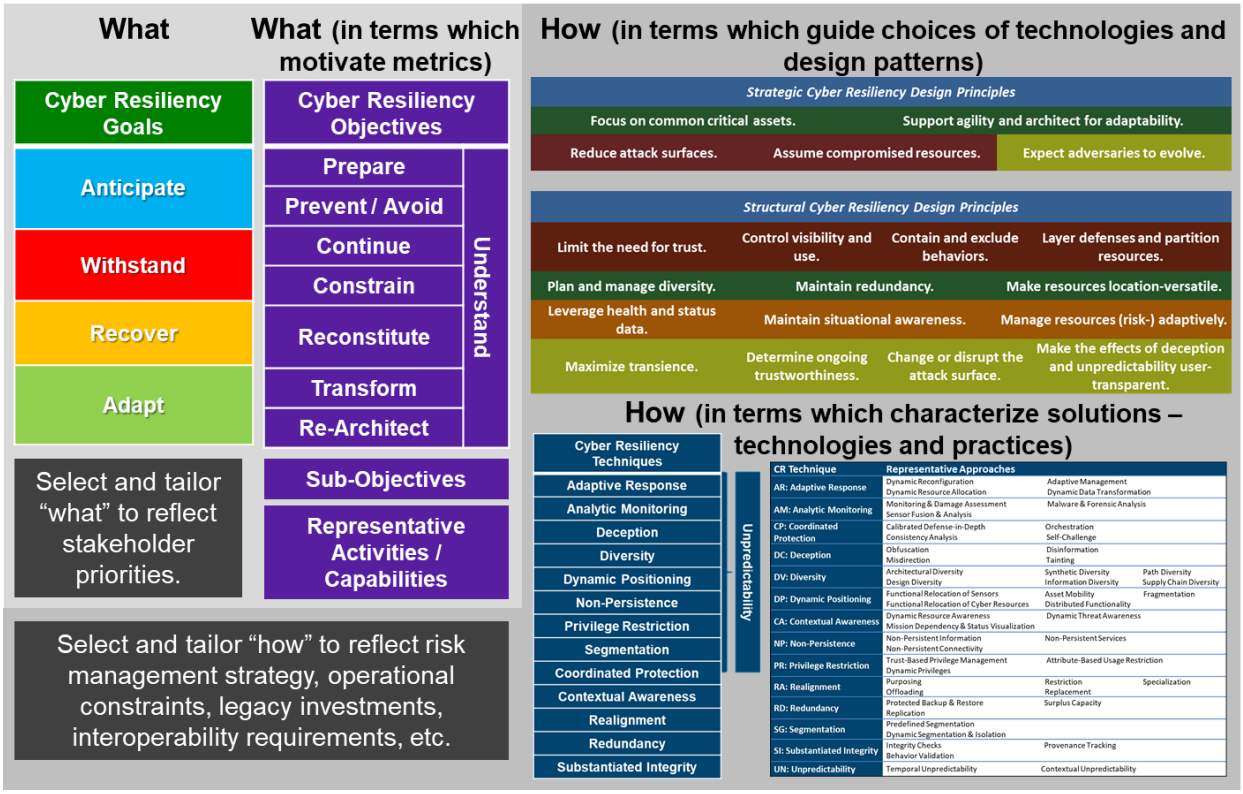

Figure 3. Overview of the Cyber Resiliency Engineering Framework (CREF)

For definitions of objectives, design principles, techniques, and approaches, see [1]. As indicated in Figure 3, CREF constructs are intended to be interpreted for and applied selectively to systems and programs, based on a variety of practical considerations. Programmatic constraints together with the system context – including the system architecture, concept of operations, threat model – enable the definitions of "what" constructs to be interpreted in stakeholder-meaningful terms. For example, within the context of a workflow system, implemented as a constituent of an enterprise's information infrastructure, the Understand objective might be restated as "Provide error detection, error correction, and interfaces with supporting services which handle adversity." By contrast, for a campus microgrid which is a safety-critical CPS, Understand might be restated as "Maintain situational awareness of the status of system elements, patterns and predictions of use, and status of external systems (e.g., regional power grid)." The representative set of sub-objectives and activities presented in Appendix B are intended to be interpreted, selected, and tailored. Some sub-objectives or activities may need to be deleted or replaced rather than simply restated; additional sub-objectives or activities may need to be defined.

[7] The Dynamic Representation technique which appears in earlier CREF documentation has been renamed Contextual Awareness.

Similarly, the applicability of "how" constructs must be determined based on programmatic constraints and the system context. For example, while Information Diversity may be less relevant to the workflow system, it may be highly applicable to performance or health and status (H&S) data for the campus microgrid, using different analog-to-digital conversion methods to non-digitally-obtained data. A key precept underlying the CREF is that no system or program can be expected to apply all cyber resiliency design principles or techniques.

Figure 4 illustrates how the more detailed "what" constructs – sub-objectives and activities (or capabilities) – relate to the higher-level constructs of goals and objectives, and provide a link between the high-level "what" constructs and the "how" constructs of cyber resiliency techniques and implementation approaches. (Representative sub-objectives and activities are defined in Appendix B of this report.)

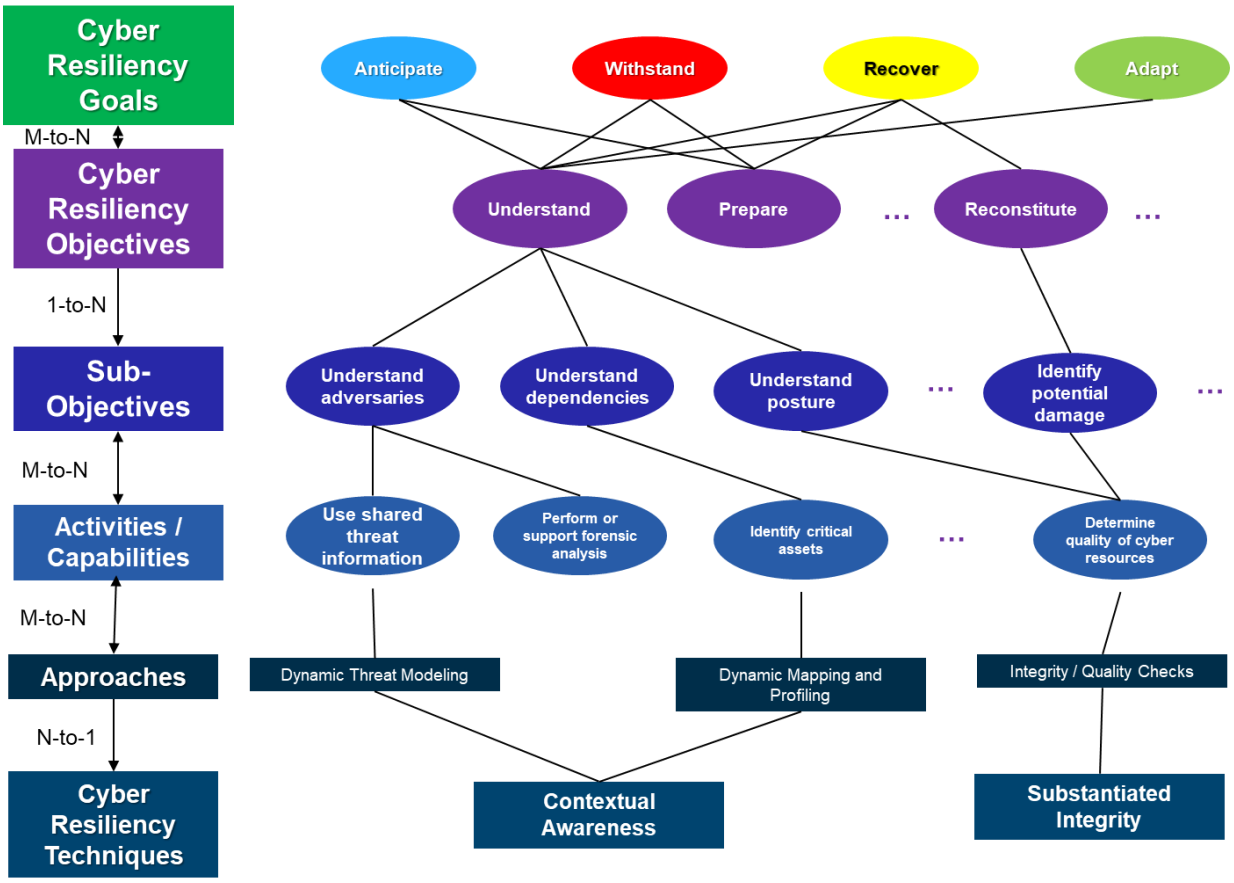

Figure 4. The CREF Provides Traceability Between the "What" and the "How" of Cyber Resiliency

The number and variety of CREF constructs is a consequence of the many possible contexts in which cyber resiliency is needed. As Figure 4 illustrates, the relationships among the constructs are often many-to-many, but traceability can be established.[8]

[8] Because objectives, sub-objectives, and activities must be selected for and tailored to a given situation, the representative mappings which can be derived from Appendix B may need to be tailored as well. This tailoring will in turn affect the selection and tailoring of corresponding metrics.

2.3 Related Types of Metrics

Cyber resiliency metrics are closely related to resilience metrics, risk metrics, and cybersecurity metrics. Many metrics defined for those specialty engineering disciplines can be re-purposed for cyber resiliency. Many of the challenges involved in defining, evaluating, and using cyber resiliency metrics are similar to those for resilience in general or for cybersecurity metrics.

As organizations recognize the need for operational resilience against breaches and distributed denial-of-service (DDoS) attacks, metrics related to contingency planning and continuity of operations (COOP) are often recharacterized as cyber resilience metrics.

2.3.1 Resilience Metrics

Resilience metrics are generally defined in the context of the disruption model illustrated in Figures 5 and 6 In this model, performance or functionality (of a system, a business function, or a sector) is mapped against time; a disruption or incident occurs, which causes performance to drop or functionality to be diminished; and performance or functionality is recovered.

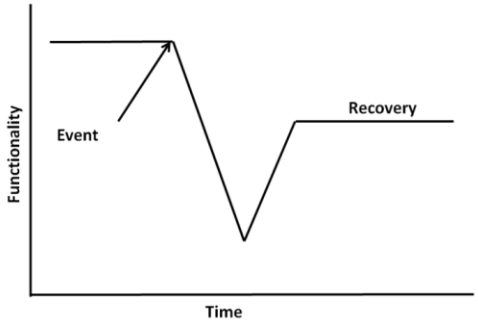

Figure 5. Disruption Model for Survivability or Resilience Engineering[9]

Variations of this model have been defined for system resilience [19], cybersecurity in general [20], and security for industrial control systems (ICS) [21]. This paper refers to such models collectively as "the reference resilience model" (or RRM).

[9] This graphic is taken from the Systems Engineering Body of Knowledge (SEBoK), http://sebokwiki.org/wiki/File:Disruption_Diagram.PNG.

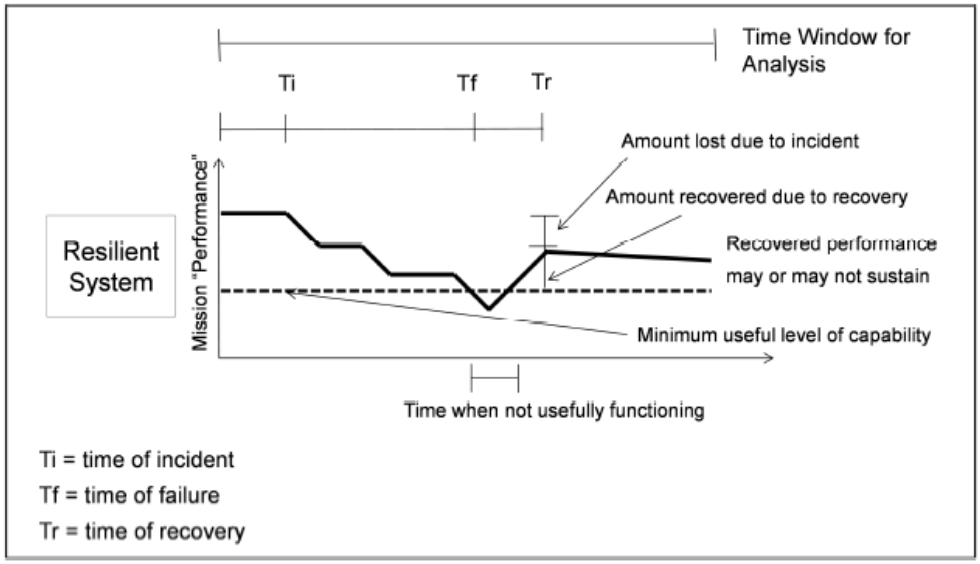

Figure 6. Performance Curve Illustrating Aspects of Resilience (Figure 1 of [22])

Metrics associated with the RRM include measures of time (e.g., between when performance degrades below an allowable threshold and when it is restored to at least that threshold) and measures of performance (e.g., the area under the performance curve from the time when performance degradation starts and the time when recovery is complete). Many of the representative metrics in [10] are based on the RRM. As noted by Cybenko [20], performance is more easily evaluated when it can be tied to measurable system properties (e.g., network throughput); levels of performance with respect to security objectives (e.g., confidentiality) are harder to define and hence to evaluate.

Metrics associated with the RRM are most easily evaluated in synthetic environments – i.e., via modeling and simulation (M&S), on a cyber range, or in a test environment – where the time of the initial disruption can be established. However, such metrics can also be evaluated in an operational environment, subject to judgment and interpretation by subject matter experts (SMEs).

Published system resilience metrics associated with the RRM focus on recovery and withstanding. Metrics related to anticipating generally are attributed to contingency planning or cyber defense; metrics related to adapting generally are attributed to cyber defense or acquisition agility. Metrics related to recovering (and to a lesser extent on withstanding) can be construed in terms of reconstituting required capabilities [23].

2.3.2 Risk Metrics

Resilience metrics are closely related to risk metrics [24]. The relationship between risk and resilience can be problematic, particularly in the complex (and socio-technical) systems considered in catastrophe management [25] [26]. However, the relationship can be usefully articulated in the case of *mission* resilience and *mission* risk [22]. In that case, cyber resiliency is a key aspect of mission resilience, and cyber resiliency metrics relate to mission risk metrics. Because cyber resiliency is predicated on the assumption that compromises will occur, many cyber resiliency metrics focus on the consequence aspect of the conventional security risk model (risk as a function of threat, vulnerabilities or predisposing conditions, and consequences [27]). Therefore, cyber resiliency metrics depend on the ability to determine the mission impacts of cyber adversity [28] [29] [30] [31].

2.3.3 Information Security or Cybersecurity Metrics

Information security or cybersecurity[10] metrics for systems or systems-of-systems can often be repurposed as metrics related to the Prevent / Avoid and Understand cyber resiliency objectives. See [32] [33] for surveys of the security metrics literature. The need for cybersecurity metrics at all scales has long been recognized as a research challenge [34] [35] [36] [37].

Many organizational security metrics have been defined, related to organizational conformance to standards of good practice; these include FISMA metrics [38] and the Center for Internet Security (CIS) Security Metrics [39]. A report on organizational use of security metrics observes that the most common purpose is demonstration of compliance or conformance with good practices [40].

Organizational security metrics related to the identification, assessment, and closure of vulnerabilities are also common [41]. Cybersecurity metrics for software include number of defects found and number of interfaces (i.e., size of software attack surface); software security metrics can also be related to risk metrics [42].

Scoring systems for different aspects of information security or cybersecurity have also been developed; see Section 5 below for more information.

2.3.4 Organizational Resilience Metrics

The term "cyber resilience" is being used by many organizations today to refer to organizational resilience against cyber incidents, breaches, and DDoS attacks [43] [44]. Thus, many cyber resilience metrics at the organizational scale are oriented toward a combination of good cybersecurity hygiene and incident response. For example, the 47 metrics in the cyber resilience metrics library published by the Shared Research Program (SRP) Cyber Security [45] are specified in terms of ten capabilities: avert social engineering, engage threat intelligence, address vulnerabilities, handle cyber incidents, resist malware, resist system intrusions, resist DDoS attacks, protect credentials, protect key assets, and measure and minimize damage. The 46 metrics defined by the Security and Industry CERT [46] are grouped by the cyber resilience goals; for example, metrics for Anticipate are in the areas of cybersecurity policy, risk management, and cybersecurity training. Discussions of cyber resilience metrics in the sense of organizational resilience (e.g., [47] [48]) generally omit the architectural, engineering, and programmatic aspects, which are the focus of the CREF and of the metrics discussed in this publication.

2.3.5 Common Challenges

A number of challenges in defining, evaluating, and using metrics are common to the closely related domains of cyber resiliency, system resilience, and cybersecurity. These include the quest for a single figure-of-merit, the problem of identifying observables, and composability Discussion of challenges related to scoring systems is deferred to Section 5 below.

2.3.5.1 Complexity vs. a Single Figure-of-Merit

A quantitative *single figure-of-merit* for resilience or cybersecurity in general is often identified as desirable, and similarly a single figure-of-merit is often desired for cyber resiliency. One figure that has been recommended is expected availability of required capability [49], with the caveat that additional metrics may need to be specified separately to address other aspects. To support engineering decisions, any single metric will either obscure the complexity of the problem domain or require a large number of

[10] See Appendix E, Glossary, for definitions of security, information security, and cybersecurity. The relationships among these domains and between these domains and cyber resiliency continue to evolve, as technology and its uses evolve (in particular, Internet of Things (IoT) and "smart" entities, from Smart Grid to Smart Transportation to Smart Cities).

input measurements, which can vary so much in quality (e.g., timeliness, accuracy) that the resulting figure is highly uncertain.[11] [10]

To do justice to complexity, formulas and models that produce a single figure-of-merit represent large sets of possible adversities and potential consequences. [50] [22] [51] [52] [53] [54] In M&S environments, these are tractable computationally and in terms of being able to supply input values of a consistent level of quality. [55] [56] [29] [30] [57] In addition, M&S enables determination of sensitivity to input values and assumptions. M&S can be used to produce visualizations of mission risk and resilience, under stated assumptions, to compare alternative solutions [22] [58].

Outside of M&S environments, complex formulas and models provide value as subjects of discussion among stakeholders and engineers, to clarify assumptions about what matters. Effectively, the formulas act as "boundary objects." [59] [60] [54] However, obtaining quality (e.g., timely, consistent) information at a reasonable cost presents significant challenges. In addition, the threat models may fail to represent actual adversaries, may be based on stale information about adversary TTPs, or may be based on information about adversary TTPs which the adversary has deliberately manipulated.

2.3.5.2 Comparability

Comparison of metric values – across organizations, between organizational units with different missions or business functions, or over time – also presents challenges. Within a sector – i.e., among organizations with similar missions or business functions, which face common threats and to which similar standards of good practice apply – comparison of organizational metrics can be meaningful and informative, if those metrics are evaluated in a consistent manner across the organizations. However, such consistency is often difficult to achieve (or to demonstrate). Different missions (and the systems or systems-of-systems which support those missions) face different threats and are executed in different operational environments. Thus, a metric which is meaningful and useful in the context of one mission may not be meaningful or evaluable in the context of another. Metric values tracked and compared over time for the same organization, mission or business function, or system can be useful to identify trends. Beyond that, comparison becomes more challenging, and must be situated in a common threat and operational context to be meaningful.

Cybersecurity and cyber resiliency metrics can vary widely in the level of detail with which the threat model will be defined or assumptions about the threat will be stated. Many metrics assume assumes a high-level threat model, while MOEs for alternative solutions are more reliant on specific threat models (e.g., descriptions of representative attack scenarios, identification of specific threat events).[12] For metric values to be comparable, the threat models assumed or explicitly represented in the metric evaluation processes need to be consistent.

Similarly, metrics vary with respect to assumptions about the operational environment as well as the level of detail with which the operational environment is represented. That is, metric values are sensitive to the metric evaluation environment [36] [16]. Metrics evaluated in different environments, even if defined in the same way, may be incomparable.

---

[11] This is the case even when the figure-of-merit is ordinal: "… resilience is not a 1-dimensional quantity." [17] As captured in MITRE's CREF documentation [5] [4], stakeholder goals and objectives, as well as the techniques that can be brought to bear to improve cyber resiliency, vary significantly depending on a number of political, operational, economic, and technical (POET) factors.

[12] Note that a common threat modeling framework can be used to develop both an enterprise-specific threat model and threat models for organization-spanning missions or systems-of-systems [86]. Use of a common framework can aid in comparison.

2.3.5.3 Composability and Emergence

Security, resilience, safety, and cyber resiliency are all types of emergent system properties [2]. While resilience can be a property of a device or platform [61], when system elements are assembled into increasingly complex systems and systems-of-systems, new properties and behaviors can be expected to arise:

> "Emergence and complexity refer to the appearance of higher-level properties and behaviours of a system that obviously comes from the collective dynamics of that system's components. These properties are not directly deductable from the lower-level motion of that system. Emergent properties are properties of the "whole" that are not possessed by any of the individual parts making up that whole." [62]

Metrics for any type of emergent property present challenges with respect to how, and how well, metrics for the properties or behaviors of system elements or subsystems can be composed – aggregated, "rolled up," or otherwise used to derive metrics for the larger system or system-of-systems.

Emergence presents challenges for defining cyber resiliency metrics. "*Emergent properties* are typically qualitative in nature, are subjective in their nature and assessment, and require consensus agreement based on evidentiary analysis and reasoning." [2] Cyber resiliency metrics express, or provide evidence to support, assessments of cyber resiliency as an emergent property. The relationship between the metrics – observables, atomic measurements, or derived values – and the subjective assessments they support must be well defined. Like security, cyber resiliency arises as an emergent property of a system in an operational and threat environment – the behaviors of the system as a whole depend on behaviors of system users, operators, adversaries, and defenders who are part of it [63]. Thus, the definition of a cyber resiliency metric needs to identify assumptions about those environmental characteristics. Composition of individual metrics can only be meaningful when the environmental assumptions are consistent.

2.4 Characterizing Cyber Resiliency Metrics

Cyber resiliency metrics, like the cybersecurity and system resilience metrics to which they are closely related, can be characterized in a variety of ways. One approach to characterizing cyber resiliency metrics is to identify the domain in which they will be evaluated and used, together with the cyber resiliency goal for which they indicate achievement. Another approach is to characterize metrics in terms of the scope or scale at which they will be evaluated or for which they are meaningful, corresponding to the scope or scale for which cyber resiliency is sought. A third approach is to place them on a spectrum from low-fidelity to high-fidelity. Higher fidelity metrics provide more conceptional, evaluative, and analytic alignment with specific cyber resiliency goals. Finally, a framework for (conventional) resilience metrics suggests desirable characteristics for cyber resiliency metrics.

2.4.1 Cyber Resilience Matrix Framework for Characterizing Metrics

Resilience research at the US Army Engineer Research and Development Center considers resilience in a broader context than cyberspace, applying concepts related to risk analysis and environmental modeling [26] [64]. Central to that work is the observation that systems exist in four domains: physical, information, cognitive, and social. That work has been applied to the cyber realm [65] [66], including to network centric operations [67] and industrial control systems [68].

As illustrated in Table 1, this framework can be used to characterize activities which support or indicate the achievement of cyber resiliency goals in the four domains, and the corresponding *metrics*. (Note that the interpretations of the domains in Table 1 is slightly different from that in [66].) A change in the value of one or more metrics can serve as a measure of the effectiveness of a cyber resiliency solution.

Table 1. Characterizing Metrics Using the Cyber Resilience Matrix [66]

Domain	Anticipate	Withstand	Recover	Adapt
Physical	Implement physical sensors for critical components (*Percentage of critical components for which physical sensors are implemented*)	Use redundant components to continue service (*Percentage of components for which an alternative is provided*)	Restart components in known good state (*Time to complete restart*)	Replace obsolete or obsolescent components (*Percentage of obsolescent components replaced in a given upgrade cycle*)
Information / Technical	Modify system configuration based on threat intelligence (*Time to propagate modifications*)	Transfer functioning to replicated resources (*Time to complete transfer*)	Assess damage to system components (*Time needed to make damage assessment*)	Restructure systems to reduce exposure (*Size of software attack surface*)
Cognitive	Develop and exercise a cyber playbook (*Number of CCoAs which are regularly exercised*)	Select and tailor CCoA (*Time to complete tailoring*)	Restore mission-essential capabilities (*Percentage of mission-essential capabilities restored in stated time*)	Reduce unnecessary dependencies (*Percentage of mission threads with no dependencies on non-mission resources*)
Social / Organizational	Share threat intelligence with other organizations (*Number of threat sharing communities in which the organization participates*)	Reprioritize mission tasks based on status (*Percentage of mission tasks which can be reprioritized*)	Communicate status of recovery efforts to affected stakeholders (*Percentage of affected stakeholders notified*)	Restructure roles and responsibilities to improve integration of cyber resiliency, COOP, and security (*Number of roles for which shared responsibilities are defined*)

2.4.2 Scope or Scale

As illustrated in Figure 7 [7], cyber resiliency can be a desirable property across a range of scales or scopes. For each scope, a different set of metrics can meaningfully be defined and feasibly evaluated. These scopes correspond roughly to the four domains in the Cyber Resilience Matrix: components and systems which can be sensed using physical means can be assessed in the physical domain; systems and systems-of-systems which support missions can be assessed in the information or technical domain; programs, mission operations, and cyber defense operations within an organization can be assessed in the cognitive domain; and structures and mechanisms for making decisions related to cyber resiliency, at the organizational, sector, regional, national, or transnational scale, can be assessed in the social or organizational domain.

Figure 7. Scope or Scale at Which Cyber Resiliency Can Be Assessed

As indicated by the red circle in Figure 8, this report focuses on metrics for components, systems, and systems-of-systems, which can be identified with missions.[13] Note that, while Figure 8 situates a mission (and its supporting system-of-systems) within an organization, that organization can be virtual and can be identified with a mission which spans multiple established organizations. Cyber resilience metrics on a sector or regional scale are outside the scope of this report; see [69] for a discussion of such metrics.

2.4.3 The Measurement Spectrum

As illustrated in Figure 8, metrics for cyber resiliency can be characterized in terms of their fidelity – i.e., their rigor and granularity. For purposes of characterizing cyber resiliency metrics, rigor relates to conceptual rigor (i.e., the extent to which a metric is defined in terms of well-defined and generally accepted concepts or constructs), evaluative rigor (i.e., reproducibility and repeatability of the evaluation process [70]), and analytic rigor (i.e., the rigor of the analytic process which uses metric values as information)[14]. The conceptual rigor of a metric's definition is demonstrated by describing how that metric relates to cyber resiliency constructs (goals, objectives, sub-objectives, activities, or design principles), risk factors (particularly the likelihood that an adversary activity will succeed, and the severity of a threat event's impact), or a mission model. The evaluative rigor of a metric depends on its evaluation environment [16]. Analytic rigor can be supported or undermined by a metric's granularity (i.e., the number of possible values it can take). In general, quantitative values – particularly those with a high degree of granularity (e.g., multiple significant digits) – should be used only for metrics with a high degree of conceptual and evaluative rigor.

[13] A comprehensive literature review on definitions and metrics for resilience [159] identified four broad problem domains: organizational, social (e.g., psychological resilience, community resilience), economic, and engineering. Of the identified definitions and metrics, only those related to engineering are relevant to this report; in particular, metrics for social resilience beyond the individual person and for economic resilience relate to sectors or regions or beyond.

[14] As explicated by Zelik et al., attributes of rigor in information analysis processes include hypothesis exploration, information search, information validation, stance analysis, sensitivity analysis, information synthesis, specialist collaboration, and explanation critiquing; three levels of rigor can be defined [153].

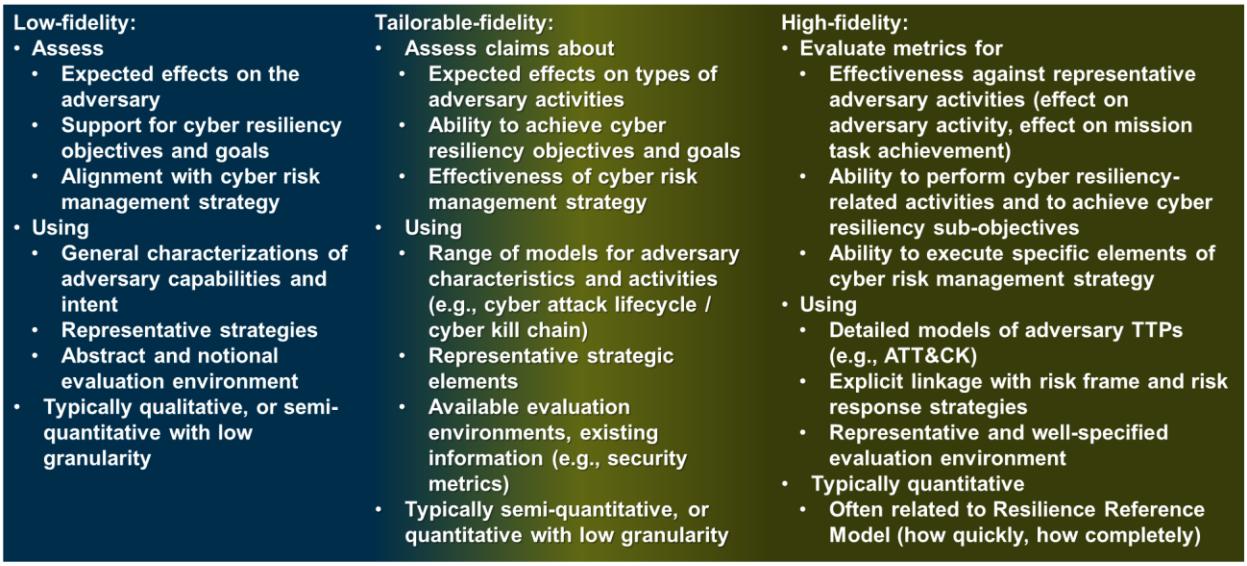

Figure 8. Measurement Spectrum for Cyber Resiliency Metrics

The three levels of fidelity represented in Figure 8 roughly track the three tiers in the proposed tiered approach to resilience assessment [9] [71] [8]. In that approach, the complexity of the model – and the associated costs to acquire, process, and analyze assessment data – depends on the intended purpose of the assessment. Tier I models are used to identify possible improvements and focus further analysis; Tier II models are used to prioritize investments; and Tier III models support detailed and complex analysis of interactions and scenarios.

The metrics identified in Appendix B and the Cyber Resiliency Metrics Catalog are intended to be elaborated into high-fidelity metrics, using the metric template in Appendix C. The topics to be covered in a metrics definition, as discussed in Section 4, enable metrics to be defined across the measurement spectrum. The scoring system described in Section 5 is low-fidelity; in the tiered approach, it is a screening model (Tier I). The metrics identified in Appendix B are intended to be evaluated in a real-world setting, but can be evaluated using detailed models (Tier II), and may be further specified to be evaluated using complex models (Tier III).

2.4.4 Types of Decisions

As Table 2 indicates, the types of decisions a metric is intended to support can drive the desirability of such characteristics as fidelity (see Section 2.4.3 above); relationship with MOPs, KPPs, or MOEs (see Appendix A); and relationship with other classes of metrics. These may include system resilience (see Section 2.3.1), risk (see Section 2.3.2), cybersecurity (see Section 2.3.3), or organizational resilience (see Section 2.3.4).

Table 2. Types of Decisions Drive Desirable Metric Characteristics

Decision Type	Examples of Decisions	Desirable Metric Characteristics
Engineering	Which solution(s) can be applied Whether a solution offers enough improvement to justify its cost	High-fidelity Relatable to system MOPs or KPPs Compatible with other technical metrics, possibly derived from the same data Relatable to cost metrics
Programmatic / Investment	Whether the cyber resiliency posture of the to-be or to-be-upgraded system is sufficient, or additional solutions should be sought Trade-offs between investments for cyber resiliency and those for other risk domains (e.g., security, safety, cost, schedule)	Low-fidelity but traceable to / supported by evidence in the form of metrics supporting other decision domains Easily understood and compared Relatable to other risk domains (e.g., value scales calibrated so that comparison across risk domains is possible)
Tactical Operations	[Mission Operations] How well a given course of action will ensure successful completion of a mission task or successful performance of a mission function; which COA to take [Cyber Operations] How effective a given cyber course of action is expected to be against the adversary; which CCoA to take	High-fidelity or tailorable-fidelity Can be evaluated dynamically, on system in its operational environment, in a timeframe that supports COA selection Relatable to mission MOEs or to MOEs for effects on adversary TTPs
Administrative / Management	Whether and how well existing capabilities and resources support cyber resiliency When and how to use existing security capabilities and contingency planning resources	High-fidelity or tailorable-fidelity Compatible with other metrics (e.g., system performance, FISMA metrics), possibly derived from the same data
COA Analysis	Whether the existing cyber playbook is sufficient, or whether it needs to be improved	Low-fidelity but traceable to / supported by evidence in the form of metrics supporting other decision domains

2.4.5 Sandia Resilience Metric Framework

A conceptual framework for developing resilience metrics was developed at Sandia National Laboratories [72]. In that framework, a notional resilience metric is a probability distribution, which maps the probability of consequence against consequence severity, as illustrated in Figure 9. A resilience metric is defined as an instantiation of that notional representation, which specifies the applicable system (where "system" is construed broadly, and includes for example a regional electrical grid), the threat, and the consequences.

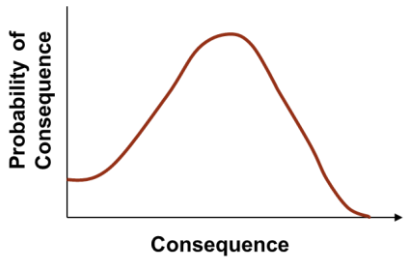

Figure 9. Resilience Framework – A Notional Resilience Metric [72]

As presented in Table 3, the core characteristics of this notional resilience metric can provide useful insights in the cyber resiliency context. However, the notional resilience metric was developed for conventional resilience, measured as probability distribution of consequence to extreme events, and for organizational use in the electricity, oil, and gas sector. As indicated in Table 2, the characteristics therefore must be adapted to apply to the cyber resiliency domain and to programs responsible for systems (including systems-of-systems), regardless of the organizational context.

Table 3. Resilience Metric Characteristics in the Cyber Resiliency Context

Metric Characteristic	Cyber Resiliency Context: A Cyber Resiliency Metric Should …
The metric is in terms of threat.	Define, or refer to a clear definition of, the threat model in the context of which the metric will be evaluated. The threat model needs to consider advanced cyber adversaries.
The metric is based on performance.	Relate the metric to mission MOPs or KPPs, cyber defense MOPs, or to performance of activities which enable cyber resiliency sub-objectives and objectives to be achieved.
The metric measures consequence.	Relate the metric to mission or organizational consequences of threat realization. The metric may not *measure* consequence (i.e., it may not be transformed into units of consequence), but if it cannot be related to mission or organizational consequences, its usefulness will be hard to defend.
The metric accounts for uncertainty.	Quantify uncertainty if and where possible. Unlike the metrics described in [72], a cyber resiliency metric may account for uncertainty in the way it is expressed (e.g., qualitative or semi-quantitative form). In a complex model of a cyber contested environment, propagation of uncertainty from multiple parameters may make quantitative results hard to defend. However, the definition of the metric can and should identify the underlying assumptions (about the context in which it is intended to be used) to which it is sensitive.
The metric effectively captures resilience.	Trace the metric to a cyber resiliency objective.
The metric is not a value judgment. [That is, it does not establish target values.]	Enable but not require the establishment of target values. Accommodate stakeholder and SME value judgments via scoring and ranking. Recognize that expert judgment is involved in the definition of any metric, by selecting parameters and thresholds, and by deciding which observables to use.
Multiple metrics are often necessary.	Specify the environment in which the metric can meaningfully and usefully be evaluated and used. If possible, related or compatible metrics should be identified.
System-level models play a key role in resilience metric computation.	Specify the system-level models (e.g., notional architectures) in which the metric can be used.

These characteristics, as interpreted, inform the Cyber Resiliency Metric Template described in Section 4.3 and included as Appendix C.

2.5 Situating Cyber Resiliency via Use Cases

Cyber resiliency analysis and metrics are sensitive to a wide variety of assumptions about the context – the operational, programmatic, and threat environments – in which alternative solutions are identified and considered.[15] As illustrated in Figure 10, these assumptions constrain the solution space as well as the

[15] The value of documenting such assumptions is addressed in the discussion of metric specification in Section 4.3 below. The Cyber Resiliency Metrics Template presented in Appendix C includes fields to be populated to document assumptions.

space of possible metrics and analysis methods.[16] That is, contextual assumptions *situate* the problem of providing cost-effective, mission- and risk-appropriate cyber resiliency.

Figure 10. Situating Cyber Resiliency Solutions, Metrics, and Analysis Methods

Therefore, the effective application of analytic methods, scoring, and metrics can best be illustrated via use cases or notional worked examples. In a use case, assumptions about the operational, programmatic, and threat environments are documented. Assumptions are reflected in restatements of such cyber resiliency constructs as objectives, sub-objectives, and activities. The relative priority of those "what" constructs is determined, as is the relative applicability of such "how" constructs as design principles, techniques, and approaches. A baseline is established for the overall cyber resiliency of the system. A representative set of alternative solutions – possible ways to improve cyber resiliency in the stated context, subject to the identified constraints – is identified and discussed in the context of those assumptions. Assessments are made of the relative improvement offered by each alternative, and cyber resiliency metrics or MOEs which could serve as evidence to support or disconfirm the assessments are identified. A companion document [12] presents the use case framework developed under the MECR project and illustrates elements of the framework for different use cases.

2.6 Cyber Resiliency Metrics Catalog

Nearly 500 representative cyber resiliency metrics have been captured in a searchable catalog, presented in a companion document [11]. Some metrics – particularly those related to the Prevent / Avoid objective – are, or are derived from, cybersecurity metrics. Others – particularly those related to the Recover goal and to the Constrain and Reconstitute objectives – are, or are derived from, system resilience metrics. In addition, a large number of metrics have been identified by defining representative sub-objectives of the cyber resiliency objectives, identifying activities or capabilities which enable those sub-objectives to be achieved, and then identifying metrics which indicate how well those activities can be performed.

[16] In practice, programmatic constraints reflect assumptions about the technical environment. The technical environment is represented separately in Figure 11 for expository purposes.

Each entry in the metrics catalog – each generic or tailorable metric – is intended to serve as the starting point for a more complete definition. A catalog entry includes identification of the cyber resiliency constructs to which it relates, the types of systems for which it can be used or tailored, the types of decisions it can be used to support, and the decision domain to which it relates. The information in a catalog entry is intended to help catalog users determine which generic metrics are potentially relevant to, and tailorable for, a specific organization or set of circumstances. A tailored metric can be more fully specified by using the Cyber Resiliency Metric Template; a complete definition may include, for example, identification of specific tools that are used to gather or process data used in the evaluation of the metric, as well as how frequently the metric is evaluated.

The Cyber Resiliency Metrics Catalog can be used in conjunction with the Situated Scoring Methodology for Cyber Resiliency (SSM-CR), as discussed in Section 5 below. It can also be used as a stand-alone resource. For example, a set of generic metrics related to a given type of system or a specific decision domain can be extracted, to serve as input to an enterprise cybersecurity and cyber resiliency metrics program, as discussed in Section 4.

3 CREF-Based Cyber Resiliency Metrics and Measures

The Cyber Resiliency Engineering Framework can be used to define metrics and measures using any one of three different starting points: objectives, techniques and approaches, or design principles.

3.1 Metrics Motivated by Cyber Resiliency Objectives

The CREF, following the example of Resilience Engineering, defines four cyber resiliency *goals*: Anticipate, Withstand, Recover, and Evolve. These goals are at a sufficiently high level as to make direct assessment of how well they are achieved subject to interpretation – and misinterpretation. As illustrated in Figure 11, the CREF therefore provides additional structure, to enable the definition of qualitative assessment scales as well as the identification of quantitative metrics which can support the assignment of qualitative values. For each CREF construct shown in Figure 11, clarifying questions (as shown on the left) can be used to elicit stakeholder concerns and priorities. Scores or qualitative assessments can provide answers to the questions on the right; quantitative metrics can serve as indicators of or evidence for those assessments, and can be tracked over time to identify trends.

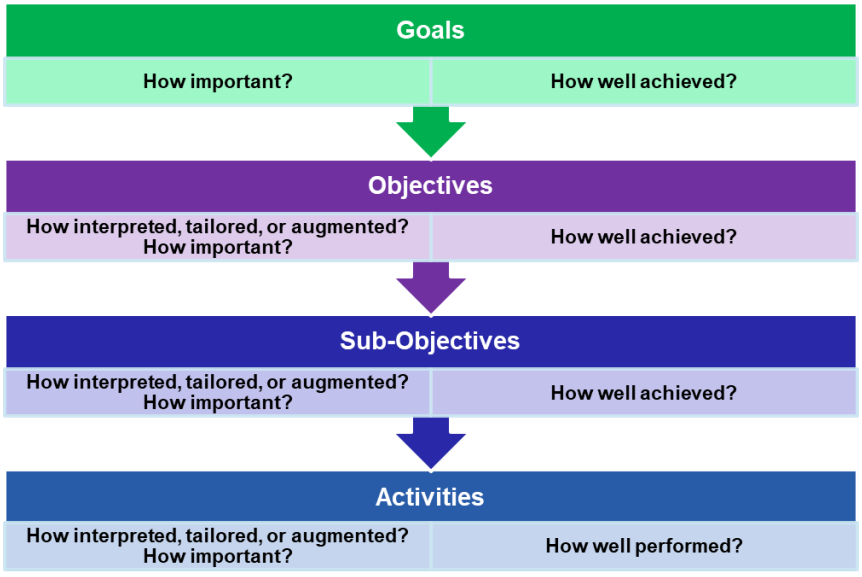

Figure 11. The Structure of the CREF Supports Definition of Metrics

At the next level below goals, the CREF defines eight high-level *objectives*. Qualitative assessment scales have been defined for achieving goals and objectives. These scales are typical of qualitative metrics, in that they rely on the expertise and interpretation of the Subject Matter Experts (SMEs) using them. Evidence to support SME judgment of how well a given objective is achieved can be found in the values (and trends in values) of quantitative metrics related to that objectives.

The CREF explicates the relationship between a quantitative metric (e.g., percentage of resources, time between one event and another) and an objective by defining cyber resiliency sub-objectives and activities. A *sub-objective* is a restatement of some aspect of an objective, focusing on a category of tasks which must be accomplished in order to achieve the objective. A cyber resiliency *activity* is an action or

function which enables one or more related cyber resiliency objectives or sub-objectives to be achieved.[17][18]

Performance metrics are most easily defined with respect to activities, and activities are more easily expressed as system requirements than are approaches or techniques. However, the technologies and processes which are needed for an activity to be feasible are represented by implementation approaches to cyber resiliency techniques. Thus, the identification of activities supports not only the definition of system requirements and performance metrics, but also the mapping between cyber resiliency techniques and objectives.

The CREF is predicated on the assumption that a foundation of security controls and continuity practices has been implemented. That assumed foundation is roughly consistent with the Moderate baseline in NIST SP 800-53 [73], and with the Framework Core of the NIST Cybersecurity Framework (CSF) [74] [75]. Therefore, a variety of activities are assumed which support cyber resiliency activities. For example, "Inventory physical devices, systems, software platforms, and applications within the organization" [69], corresponding to ID.AM-1 and ID.AM-2 in the CSF, is assumed rather than identified under the Understand objective.

Sub-objectives and activities can be identified in general or representative terms, or can be stated in terms specific to a use case. This white paper identifies a broadly representative set of sub-objectives and activities. Some of these representative sub-objectives and activities will not be meaningful or relevant to specific use cases or classes of systems. For example, for a deployed cyber-physical system (CPS) which integrates commercial off-the-shelf (COTS) components, no meaningful way may exist to harden resources based on threat intelligence (a sub-objective of the Prevent / Avoid objective), while the Re-Architect objective as a whole may be deemed irrelevant.

The structure of cyber resiliency goals, objectives, sub-objectives, activities, and metrics is illustrated in Figure 12. This structure is similar to that found in other frameworks, such as the NIST Cybersecurity Framework [75]. However, unlike the tree structure of functions, categories, sub-categories, and representative controls as defined in the CSF, the CREF uses a mixture of a tree structure and many-to-many mappings for cyber resiliency constructs (goals, objectives, sub-objectives, and activities; techniques and implementation approaches). As illustrated in Figure 12, sub-objectives and objectives, and activities and metrics, use a tree structure. However, a given objective can support multiple goals; a given activity can support multiple sub-objectives; a given approach to implementing a cyber resiliency technique can enable multiple activities; and thus, a given technique can enable multiple objectives to be achieved.

[17] A cyber resiliency activity is performed by a *system* in the sense of CNSSI 4009 [128] ("Any organized assembly of resources and procedures united and regulated by interaction or interdependence to accomplish a set of specific functions") and ISO/IEC/IEEE 15288 [139] ("Combination of interacting elements organized to achieve one or more stated purposes"), as cited in the Draft NIST SP 800-53R5. Thus, execution of a cyber resiliency activity involves some combination of people, processes, and technology. A cyber resiliency activity can be translated into a functional requirement, directly if it can be executed automatically or indirectly if it requires operator intervention; in the latter case, the corresponding requirement takes the form "shall enable [the organization | system administrators | cyber defenders | the user] to …". A cyber resiliency activity can also be identified with a nominal (yes/no) metric [67].

[18] Cyber resiliency activities were identified in the original 2011 CREF publication [6], but were associated with cyber resiliency techniques. In the 2012 revision [5], sub-objectives were defined, with accompanying qualitative value scales. The assignment of activities to sub-objectives in this current document is new; many of the activities defined in [6] have been retained, but some have been deleted, some have been reworded, and new activities have been defined.

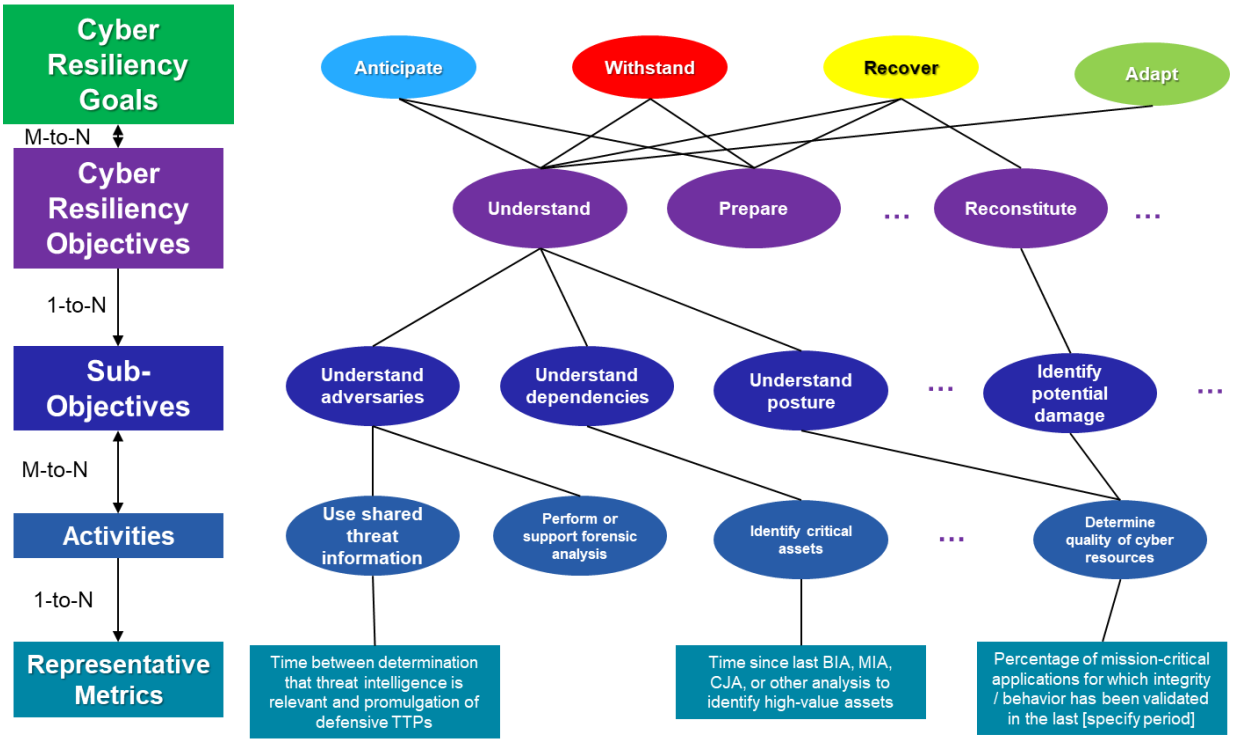

Figure 12. Representative Relationships Between Goals, Objectives, Sub-Objectives, Activities, and Metrics

Appendix B identifies representative sub-objectives, activities, and metrics for the eight cyber resiliency objectives. Representative sub-objectives are identified for each objective. For each sub-objective, one or more representative activities or capabilities are described, and the implementation approaches to cyber resiliency techniques needed to provide each capability or perform each activity are identified. For each activity or capability, one or more representative metrics are identified in Appendix B. For some sub-objectives, a "General" capability is also identified; this enables identification of metrics which best support the achievement of each sub-objective. Approaches to implementing cyber resiliency techniques which enable the representative activities to be performed, are also identified. As illustrated in Figure 4, this identification enables approaches to be mapped to cyber resiliency sub-objectives and hence to objectives.

3.2 Metrics Driven by Cyber Resiliency Techniques and Approaches

Metrics can also be defined by considering the cyber resiliency techniques and approaches. Metrics related to techniques and approaches typically serve to answer questions of the form "how well is this approach applied?" or "how broadly is this approach applied?"

Each technique can be applied and each approach can be taken at one or more architectural layers. However, because the implementation approaches to cyber resiliency techniques are more specific than the techniques, many approaches are not useful (or even feasible) at all architectural layers. Questions of the form "how broadly" can focus on whether the approach is applied at all potential architectural layers, or on whether the approach is applied to all system elements within a given architectural layer. For example, one metric for Architectural Diversity is the percentage of layers for which Architectural Diversity is an option to which this approach has actually been applied – at how many of those layers are architectural alternatives actually provided? Another metric focuses at the operating system layer: how

many different architectural alternatives (e.g., Windows-based, Linux-based) are provided at that layer? Many implementation approaches are mapped to a set of architectural layers in [5].[19]

Questions of the form "how well" are posed and answered in an assumed context of a defined threat model, system concept, or programmatic strategy. In particular, "how well" metrics are often related to effects on adversary activities ([1], Appendix I; [76]).

The analysis to identify objective-driven cyber resiliency metrics includes, for each activity or capability, identification of the cyber resiliency techniques and approaches which enable that capability to be provided or that activity to be performed. See Appendix B for details.

3.3 Metrics Driven by Cyber Resiliency Design Principles

Cyber resiliency design principles, as illustrated in Table 4, are described in [1] [3]. As discussed by Ricci et al. [77], design principles can be characterized as (i) *strategic* to be applied throughout the systems engineering process, guiding the direction of engineering analyses, or (ii) *structural* – directly affecting the architecture and design. For a given system, only a subset of the design principles will be relevant – strategic design principles must be consistent with the risk management strategy of the program, system owner, or mission owner, while structural design principles must align with the relevant strategic design principles, as well as with design principles from allied disciplines. Appendix D provides value scales for scoring the relevance of design principles.

Table 4. Representative Cyber Resiliency Design Principles

Strategic Cyber Resiliency Design Principles		
Focus on common critical assets.		**Support agility and architect for adaptability.**
Reduce attack surfaces.	**Assume compromised resources.**	**Expect adversaries to evolve.**

Structural Cyber Resiliency Design Principles			
Limit the need for trust.	**Control visibility and use.**	**Contain and exclude behaviors.**	**Layer and partition defenses.**
Plan and manage diversity.	**Maintain redundancy.**		**Make resources location-versatile.**
Leverage health and status data.	**Maintain situational awareness.**		**Manage resources (risk-) adaptively.**
Maximize transience; minimize persistence.	**Determine ongoing trustworthiness.**	**Change or disrupt the attack surface.**	**Make unpredictability and deception user-transparent.**

Key to Aligned Disciplines:

Security	*Resilience Engineering & Survivability*	*Evolvability*	*Unique to Consideration of Advanced Cyber Threats*

For each structural design principle, metrics can be defined to assess the *extent* to which the design principle is applied or the *quality* of its application. Metrics describing the *extent* to which a structural design principle is applied typically take the form of percentages. Metrics describing *how well* a structural design principle is applied typically take the form of time to perform some action, and thus are closely related to metrics derived from objectives, sub-objectives, and capabilities or activities. See [3] for representative examples of metrics which serve as evidence of how extensively and how well structural cyber resiliency design principles have been applied.

[19] Note that additional approaches have been defined, and definitions of techniques and approaches have been updated, since publication of [5].

4 Selecting and Specifying Cyber Resiliency Metrics

As the previous sections have described, a large number of possible cyber resiliency metrics can be identified for any given system, mission, or organization.[20] However, metric evaluation involves time and effort, and may involve investment in specialized tools to gather the necessary data.[21] Therefore, the set of metrics to be evaluated, and possibly tracked over time, must be selected carefully. This section discusses considerations for identifying metrics for organizational use, as illustrated in Figure 13.

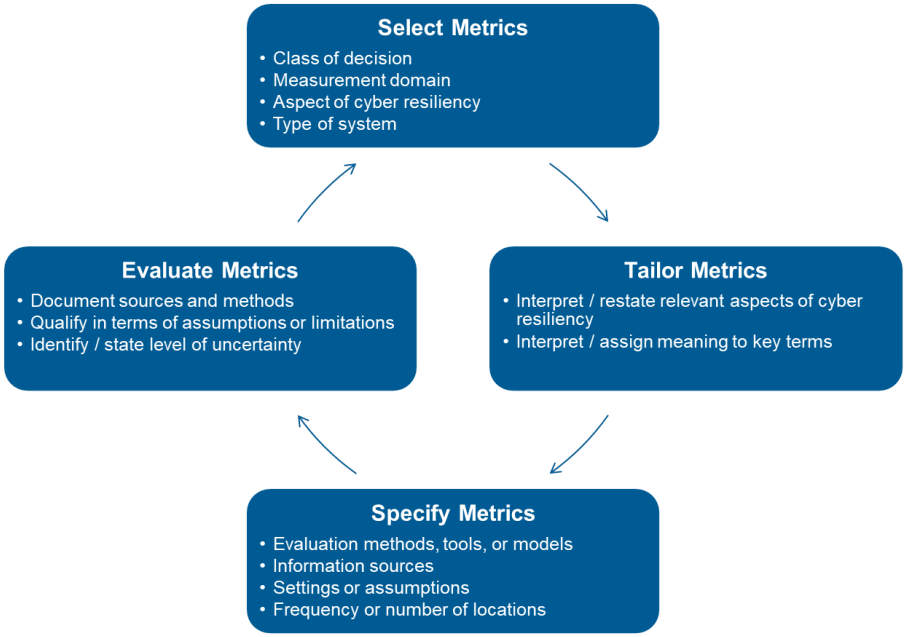

Figure 13. Cyber Resiliency Metrics Program Concept of Use

The first sub-section identifies possible criteria for selecting metrics as candidates for inclusion in a metrics program. Once a metric has been selected, it must be tailored and specified in sufficient detail that it can be evaluated in a reproducible and repeatable way. The second sub-section discusses tailoring, while the third sub-section describes the information needed in a metric specification, which is captured in the Cyber Resiliency Metric Template in Appendix C. Note that the process of tailoring and specifying a candidate metric may reveal that it is not evaluable. Evaluation is as defined by the metric specification and is not discussed in this section; see the relevant portions of the Metric Template.

4.1 Metric Selection

Multiple criteria can be considered when selecting cyber resiliency metrics, described at a high level (e.g., via a short phrase), for possible inclusion in a metrics program. First and foremost, a metric must be evaluable: it must be possible to obtain the needed data, observations, or evidence, in a timely manner, and at a cost which does not outweigh the potential benefits of understanding and decision support which

[20] A *metrics program* is a a program element within a larger acquisition or organizational program which defines, evaluates, tracks, and reports on metrics to inform decisions. Note that a metrics program typically tracks metrics for multiple risk or problem domains (e.g., security, safety, privacy, cost, schedule) to inform trade-offs.

[21] These concerns are less significant when the metric is defined and evaluated via executable models, e.g., as artifacts of model-based systems engineering (MBSE) or as products of modeling and simulation (M&S). In these situations, the costs associated with evaluating, tracking, and comparing metrics relate more to the expertise of those doing subsequent analysis and interpretation.

the metric evaluation offers. A number of additional criteria are represented in the Cyber Resiliency Metrics Catalog, including

- The types of decisions a metric is intended to support (see Section 2.4.4).
- The measurement domain (see Section 2.4.1).
- The aspect of cyber resiliency being measured of assessed, which can be a cyber resiliency objective (or can be more specific, either a sub-objective or an activity), a cyber resiliency technique (or more specifically, an implementation approach), or a cyber resiliency design principle. See Appendix B and Appendix D.

Another important selection criterion is the type of system in which the metric can be evaluated. A system type generally captures assumptions about the system architecture (e.g., EIT vs. CPS) and governance (e.g., enterprise-internal vs. federated) which determine whether the metric is meaningful for that system type, and whether it can be evaluated. For example, metrics related to levels of trustworthiness or user privilege attributes are not meaningful in a federated environment, since different organizations will define these differently; evaluation of metrics in a federated system can involve information sharing across organizational boundaries.

An additional possible selection criterion is the context in which the metric is meaningful. The threat context can include the type(s) of threat events for which a change in the metric value indicates an effect, and the type(s) of effect indicated. The operational context can include the physical environment, the human environment, and the cognitive environment in which the system operates. This selection criterion requires some judgment to apply properly; it cannot easily be automated. The Cyber Resiliency Metrics Template provides multiple fields which can be used to capture this contextual information in more detail. For the other selection criteria, the Cyber Resiliency Metrics Catalog provides searchable fields.

These selection criteria may be prioritized, for example based on organizational risk framing.

4.2 Metric Tailoring

Metric tailoring ensures that the metric, as briefly identified by a short phrase or descriptor, is meaningful in the context of a system or an organization. Tailoring involves providing definitions of key concepts and terms, so that the meaning of the metric is unambiguous, or so that aspects of the metric which require more detailed specification are identified.

Many cyber resiliency metrics are traceable to the "what" cyber resiliency constructs (objectives, sub-objectives, and activities). As noted in Section 2.2, these constructs must be restated or interpreted in the context of the system or organization. The representative set of sub-objectives and activities identified in Appendix B are intended to serve as a starting point only. Some sub-objectives may assume conditions that do not hold (e.g., continuous network connectivity), while many activities assume central governance (e.g., activities related to privilege management) or a team of cyber defenders. Once the constructs to which a cyber resiliency metric traces are restated or interpreted, the short phrase or descriptor that identifies the metric may need to be restated.

In addition, the terms and phrases in a metric descriptor need to be interpreted in the context of the system architecture and the operational concept. For example, many metric descriptors in Appendix B refer to "resources" or "data assets." While definitions are offered in the Glossary of this report, metric tailoring can provide representative examples. Other metric descriptors use the phrase "mission-critical," which implies human judgment. During tailoring, references for organizational standards or processes related to such phrases can be identified, or the need to provide more details in the metric specification can be flagged.

4.3 Metric Specification

In order for a cyber resiliency metric to be evaluated in a reproducible and repeatable way, it must be defined with more specificity than with a simple descriptive phrase. A template for characterizing cyber resiliency metrics was presented in [10], based on prior work by NIST [78], the Cyber Security and Information Systems Information Analysis Center (CSIAC, formerly the Information Assurance Technology Assurance Center or IATAC [79]), and CERT [80]. The template in Appendix C extends that template, based on

- Work characterizing cyber resilience metrics by goals and measurement domains [66] [65] [67], as described in Section 2.4.1;
- The extension of the conventional resilience reference model (RRM) to the cyber domain [68] [64] [20];
- Work characterizing cyber adversary activities, including ATT&CK™ [81], the ODNI Cyber Threat Framework [82], the NSA/CSS Cyber Threat Framework [83], and on threat modeling more broadly [84] [85] [86];
- The Vocabulary for Describing Effects on Adversary Activities (VODEA, [76] or Appendix I of [1]); and
- The evolution of the CREF [6] [4] to include cyber resiliency design principles (CRDP, [3]) as well as cyber resiliency goals, objectives, and techniques.

Topics to be addressed in a cyber resiliency metric specification include (see Appendix C for more details):

- Descriptor: A brief description (a short phrase which suggests the form of the metric, e.g., percentage, time, degree).
- Cyber resiliency properties being measured, which can include how well a cyber resiliency goal or objective is achieved or how well a cyber resiliency design principle or technique is applied.
- The type(s) of system to which the metric applies or for which the metric is meaningful. As noted in Section 4.1, a given metric may be meaningful or evaluable only for a specific type of system (e.g., EIT, CPS).
- Intended uses (e.g., as described in Section 4.1).
- Form of the metric: the type of measurement scale (nominal, ordinal, cardinal, interval, or ratio), range or set of allowed values, and units. The form of the metric is often implicit in the descriptor.
- Evaluation:
    - How is the metric evaluated? Is it measured, using hardware or software tools? Is it observed, by an individual or a team? Is it computed or derived, based on measurements or observations? Or is it judged, by an individual SME or a team of SMEs?
    - In what environment is the metric evaluated [16]? Is the evaluation conceptual (i.e., in the minds of SMEs), does evaluation result from modeling and simulation, is evaluation performed in a test environment (e.g., a laboratory, a cyber range), or is the metric evaluated in an operational setting?
    - Where, architecturally, is the metric evaluated? For a metric evaluated other than conceptually, data is collected at one or more specific architectural layers or locations.

- How often or in what timeframe (e.g., hourly, daily, monthly; over the course of a mission execution; over the course of a mission task) is the evaluation performed?

In addition, the specification of a cyber resiliency metric can include information about:

- Related cyber security or cyber defense MOPs.
- Adversary behaviors (e.g., TTPs, threat events) against which the metric measures effectiveness.
- Effects on adversary activities. These can be described using VODEA ([76] or Appendix I of [1])
- Related mission MOPs.

As discussed in Appendix A, such information can help determine whether and how the metric can be used as or in a measure of effectiveness.

5 Cyber Resiliency Scoring

Program Managers and systems engineers need support for decisions about whether the cyber resiliency properties or capabilities provided by a system are sufficient, how much they could be improved, and how those improvements relate to other possible improvements (e.g., in security, privacy, or safety). While security scoring systems can provide useful decision support to Program Managers, those systems do not address cyber resiliency. The Situated Scoring Methodology for Cyber Resiliency[22] (SSM-CR) is a tailorable scoring methodology intended to provide Program Managers with a simple relative measure of how cyber resilient a given system is, and of whether and how much different alternatives change that measure. This section provides background on scoring methodologies, with an emphasis on security scoring. SSM-CR is then briefly described; details can be found in Appendix D.

5.1 Background on Scoring Systems

Scoring systems in general are widely used to support decisions, make comparisons, and support decisions. A large literature exists for scoring rubrics and rating scales in education [87], discussing issues of fairness, rater subjectivity, and the extent to which scores are predictive of future performance [88]. A similar literature exists for credit scores, discussing issues with fairness (e.g., the use of surrogate or highly correlated factors which encode bias [89]) and aggregation (e.g., scoring portfolios). Scoring systems for sports and athletic competition are less well studied, but issues of relative priority [90] and the role of SME bias [91] are well recognized.

Security scoring and rating systems have been defined for organizations, configured products, systems, vulnerabilities, weaknesses, and incidents. Scoring systems for organizations include FISMA grades based on agency self-reporting, scores based on the Top 20 from the Center for Internet Security (CIS), and commercially provided scores for organizations based on publicly observed information [92] [93] [94] [95] or information supply by the organization itself [96] [97]. Microsoft has created a security score for Office 365 and Windows [98]. Security information and event management (SIEM) products for systems and networks produce scores (e.g., [99] [100] [101] [102]), while some offerings assess attacker resistance [103]; these offerings frequently rely on proprietary data or algorithms.

The Electric Power Research Institute (EPRI) has developed a framework for cyber security metrics and scoring [104]. At the top level, three strategic scores are defined (for Protect, Detect, and Respond); at the next level, ten tactical scores for specific security measures (e.g., endpoint protection); at the next (operational) level, 45 quantitative metrics are defined; and at the bottom level, data points to be used in evaluating the quantitative metrics are identified. The EPRI definitions take advantage of the common missions, architectures, and technologies for electric utilities. As the types of strategic and tactical scores indicate, these metrics relate primarily to conformance with cyber security best practices, rather than to attack scenarios involving advanced cyber threats with persistence.

Scoring systems related to security standards include

- The Common Vulnerability Scoring System (CVSS) [105], related to the Common Vulnerabilities and Exposures (CVE) effort. A CVSS score for a vulnerability is computed in the range 0.0 – 10.0, with a margin of 0.5. In CVSS, three groups of metrics are defined: base, temporal, and environmental. These metrics are scores, determined by selection of qualitative or nominal values. Base metrics reflect a vulnerability's exploitability, scope, and potential impacts of exploitation. Temporal metrics reflect "the current state of exploit techniques or code

[22] SSM-CR is so named because the overall process and the structure of the scoring system can be adapted to other specialty domains such as security (e.g., using the functions, categories, and subcategories of the NIST Cybersecurity Framework Core [75] rather than the cyber resiliency objectives, sub-objectives, and activities).

availability, the existence of any patches or workarounds, or the confidence that one has in the description of a vulnerability." Environmental metrics enable the CVSS score to be customized.

- The Common Weakness Scoring System (CWSS) [106], related to the Common Weakness Enumeration (CWE) effort. A CWSS score for a software weakness is computed in the range 0.0 – 100.0. In CWSS, three groups of metrics (evaluated on a scale of 0-100) are defined: base finding, attack surface, and environmental. Base finding metrics are intended capture the inherent risk of the weakness, confidence in the accuracy of the finding, and strength of controls. Attack Surface metrics assess the barriers that an attacker must overcome in order to exploit the weakness. Environmental metrics reflect characteristics of the weakness that are specific to a particular environment or operational context. CWSS supports multiple scoring methods: targeted, generalized, context-adjusted, and aggregated. Context-adjusted scores enable mission or business priorities, threat environments, and risk tolerance or risk management strategies to be explicitly considered.
- The National Cybersecurity and Communications Integration Center (NCCIC) Cyber Incident Scoring System (NCISS) [107], related to the Cyber Incident Severity Schema (CISS). NCISS produces scores in the range 0 – 100, and uses the Office of the Director of National Intelligence (ODNI) Cyber Threat Framework (CTF) [82] to characterize observed activity.

Security scoring systems which are part of cybersecurity risk analysis tools are surveyed in [108]. A multicriteria framework for cybersecurity risk assessment, including a weighted scoring system, is provided by [109].

All scoring systems, whether for security or for other purposes, are inherently problematic in a variety of ways. Algorithmic bias can arise from the selection of factors as well as from prioritization or weighting schemes. SME bias can affect the values of weights and assessed factors, while automatically obtained input data is sensitive to data-gathering tools. Any scoring system encodes assumptions about the environment or context in which scores are evaluated. Performance assessment (particularly in the absence of statistical data) reflects SME judgment, and predictive uses of scores are often undermined either by algorithmic bias or by changes in the environment or context. Differences in environment or SME background can make aggregation (e.g., scoring a portfolio, team, or sector based on individual scores) uncertain. A lack of transparency about selection of factors, weighting, input data, and assumptions can make some scoring systems more subject to challenge.

5.2 SSM-CR

This section provides a brief overview of SSM-CR, as an example of a cyber resiliency scoring system. Details are presented in Appendix D.

SSM-CR scoring has two key facets – priority and performance. Relative priorities (VL-VH, rated as 1-5, with 0 for Not Applicable) are assigned to cyber resiliency objectives, to sub-objectives (or methods for achieving objectives) for applicable objectives, and to activities or capabilities for achieving applicable sub-objectives. The assignments are based on stakeholder concerns; the objectives, methods, and capabilities are restated (tailored) for the specific system or program.

Similarly, the degree of performance, rated on a scale of 0-5, is assessed for each relevant capability, based on SME judgment (typically systems engineers supporting the Program Office), supported where possible by evidence (documentation, indicator metrics). The performance assessments are made in the context of the operational context (e.g., assumptions about the cyber security and cyber defense capabilities of users, maintenance staff, and the owning organization), the programmatic context (e.g., lifecycle stage, constraints on architecture or technologies), and the threat context. The threat context includes characteristics of cyber adversaries (e.g., motivation, goals, expertise, resources) as well as their behaviors (e.g., attack scenarios, representative events or TTPs) [84] [86].

The performance assessments for the individual activities or capabilities which support achieving a sub-objective, weighted by the activities' relative priorities, are rolled up to a performance assessment for the sub-objective. Similarly, the performance assessments for sub-objectives, weighted by relative priority, are rolled up to a performance assessment of the objective. The performance assessments for objectives, weighted by relative priority, are rolled up to produce the overall cyber resiliency score. The output of the analysis is a score in the range of 0-100, reflecting how well the system meets its priority-weighted cyber resiliency objectives in the assumed threat environment and operational environment. The score is deliberately *situated* in this context; scores from different programs are not directly comparable.

This scoring system has two key features:

- *Relationship to other metrics.* SSM-CR is designed to facilitate identification of cyber resiliency metrics or MOEs which can serve as evidence for score values. Evaluation of the scores is performed by cyber resiliency SMEs and Systems Engineers, based on consultation with stakeholders and on examination of available evidence. That evidence can include cyber resiliency metrics or MOEs evaluated in a test or operational environment. In principle, one or more metrics can be identified for each relevant capability or activity. In practice, because evaluation of such metrics can be time-consuming and costly, a small number of indicator metrics are likely to be used in conjunction with other evidence (e.g., system documentation).
  The overall structure of SSM-CR (top-level and second-level scores, more specific metrics) is similar to that of the EPRI metrics. However, SSM-CR only identifies potential metrics which could be used as evidence to support performance assessments; it does not use these computationally. This is due to the fact that SSM-CR is intended to cover a wider range of types of systems, missions, and programs. In addition, SSM-CR is intended to be used with respect to identified threat scenarios involving advanced cyber adversaries, rather than in a general cyber security context.
- *Situated scoring.* The scoring is *situated* with respect to the system's operational, programmatic, and threat context. Cyber resiliency constructs are tailored to reflect the mission, system context of use, and programmatic constraints, creating a situation-specific set of weights. Performance scores are evaluated with respect to the assumed threat model, which includes adversary goals and expected TTPs. Thus, the Cyber Resiliency Score for one system or program is not comparable with that for another; it is not a FICO cybersecurity score [92]. Rather, the score represents an assessment of how well the system or program achieves its own cyber resiliency goals and objectives. Evaluation of the Cyber Resiliency Score for a system baseline, and then for one or more potential cyber resiliency solutions, enable comparison of the expected degree of improvement each solution offers, relative to the baseline. In this respect, SSM-CR resembles context-adjusted scoring in CWSS.

While SSM-CR addresses many of the issues identified above, some challenges remain. These are summarized in Table 5.

Table 5. How SSM-CR Addresses General Issues with Scoring

Issue Area	How Addressed	Residual Challenges
Selection of factors	Derived from CREF (objectives, sub-objectives, activities / capabilities) Tailorable – selected elements are restated in the context of the system's operational and threat environments	Sensitivity of tailoring to practicioner understanding of system, environment, and cyber resiliency
Prioritization / weighting	Simple scale (0-5), assessment supported by rationale Alternative approaches (e.g., Balanced Scorecard, Analytic Hierarchy Process (AHP) as in Crown Jewels Analysis (CJA, [110])) add complexity, but could be substituted	Elicitation of stakeholder priorities and sensitivity to stakeholder biases Ensuring that weights are assigned consistently
Performance assessment	Simple scale (0-5), assessment supported by rationale Changes in assessed value (particularly large changes) drive identification of potential MOEs, to be evaluated in lab, test, or operational setting	Engineers' pushback on simple scale Sensitivity to practicioner expertise / experience Sensitivity to assumptions – need to ensure that SMEs keep operational and threat environments in mind while assessing
Underlying environmental assumptions	Use Case approach entails documenting system use concept, programmatic concept, and threat model	Sensitivity to practicioner expertise
Predictive uses	Not designed for prediction / risk assessment	Need to prevent misuse / misinterpretation
Aggregation	Scoring is explicitly situated – scores for one system / program are not intended to be comparable to scored from another – although overall assessment does indicate how well the system (or some alternative) compares with the system-specific, program-specific ideal	Need to prevent misuse / misinterpretation

Most importantly, while SSM-CR scoring does provide a way to compare alternative solutions, this comparison is quite coarse. The need remains for a scoring, ranking, or rating system intended to support systems engineers rather than Program Managers, to make detailed comparisons between alternative potential requirements, capabilities, or solutions. Such a system might make use of value scales similar to those used by SSM-CR.

6 Conclusion

This paper has extended prior work on cyber resiliency metrics [10], focusing on metrics which can be used by systems engineers and program managers to inform analysis of alternatives. It defines a scoring system and describes the different perspectives from which cyber resiliency metrics and measures of effectiveness can be defined: programmatic, engineering, mission assurance, and risk management. It identifies a large number of possible metrics, traceable to cyber resiliency objectives. It provides guidance on selecting, tailoring, and specifying metrics, including a metric template. This paper serves as a general resource for those who seek to define and use cyber resiliency metrics in a reproducible, repeatable way.

Numerous challenges remain in the cyber resiliency metric problem domain. As briefly sketched below, these include enabling comparison, defining metrics which can be combined computationally, and creating a scoring system which systems engineers could use to compare alternative solutions in detail.

- Comparison of metric values, whether across organizations or across programs or systems, requires consistency in assumptions about the context in which the metric is meaningful, as well as in evaluation methods. Model-based systems engineering can capture some assumptions and be used to compute values of model-based metrics, but work is needed to determine the limitations of this approach and to develop practical guidance. One possible building block could be a common framework for characterizing adversaries (e.g., as in [86]).

  A single figure-of-merit (e.g., a FICO-like score) which enables comparison has great attractiveness to those who must consider cyber resiliency at the level of a critical infrastructure sector, a region, or a set of organizations collectively performing a mission or business function. However, such scores have known risks, including failure to consider variations in organizational size or mission, reliance on standards of practice or threat models which can rapidly go stale, and support for a compliance (rather than risk management) mindset [93].

- The problem of combining cyber resiliency metrics for sub-systems, systems, and systems-of-systems supporting missions or business functions is similar to that for security metrics, and metrics for other areas in which system properties and behaviors are emergent. Research into risk modeling for complex systems (e.g., [111]) may be highly relevant.

  Another direction for investigation involves combining metrics across either of the dimensions of the Cyber Resilience Matrix (Table 1), i.e., across all cyber resiliency objectives viewed from a given domain (physical, information / technical, cognitive, or social / organizational), or across all domains for a given cyber resiliency goal (anticipate, withstand, recover, or adapt).

- Systems engineers need a more nuanced scoring, ranking, or rating system than Program Managers, to make detailed comparisons between alternative potential requirements, capabilities, or solutions. Such a system could take into consideration expected effects on adversary activities (e.g., ATT&CK categories, specific TTPs), effects on other aspects of risk (e.g., level of consequence), or other factors.

7 References

[1] NIST, "Draft NIST Special Publication 800-160 Volume 2, Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems," 21 March 2018. [Online]. Available: https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft.pdf.

[2] NIST, "NIST SP 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," 15 November 2016. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160.pdf.

[3] D. J. Bodeau and R. D. Graubart, "Cyber Resiliency Design Principles: Selective Use Throughout the Lifecycle and in Conjunction with Related Disciplines," January 2017. [Online]. Available: https://www.mitre.org/sites/default/files/publications/PR%2017-0103%20Cyber%20Resiliency%20Design%20Principles%20MTR17001.pdf.

[4] D. Bodeau, R. Graubart, W. Heinbockel and E. Laderman, "Cyber Resiliency Engineering Aid - The Updated Cyber Resiliency Engineering Framework and Guidance on Applying Cyber Resiliency Techniques, MTR140499R1, PR 15-1334," May 2015. [Online]. Available: http://www.mitre.org/sites/default/files/publications/pr-15-1334-cyber-resiliency-engineering-aid-framework-update.pdf or http://www.defenseinnovationmarketplace.mil/resources/20150527_Cyber_Resiliency_Engineering_Aid-Cyber_Resiliency_Techniques.pdf.

[5] D. Bodeau and R. Graubart, "Cyber Resiliency Assessment: Enabling Architectural Improvement (MTR 120407, PR 12-3795)," May 2013. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/12_3795.pdf.

[6] D. Bodeau and R. Graubart, "Cyber Resiliency Engineering Framework (MTR110237, PR 11-4436)," September 2011. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/11_4436.pdf.

[7] D. Bodeau and R. Graubart, "Cyber Resiliency Metrics: Key Observations (PR Case No. 16-0779)," May 2016. [Online]. Available: https://www.mitre.org/publications/technical-papers/cyber-resiliency-metrics-key-observations.

[8] I. Linkov and A. Kott, "Fundamental Concepts of Cyber Resilience: Introduction and Overview," in *Cyber Resilience of Systems and Networks*, Springer, 2018, pp. 1-25.

[9] A. Kott, B. Blakely, D. Henshel, G. Wehner, J. Rowell, N. Evans, L. Muñoz-González, N. Leslie, D. W. French, D. Woodard, K. Krutilla, A. Joyce, I. Linkov, C. Mas-Machuca, J. Sztipanovits, H. Harney, D. Kergl, P. Nejib, E. Yakabovicz, S. Noel, T. Dudman, P. Trepagnier, S. Badesha and A. Møller, "Approaches to Enhancing Cyber Resilience: Report of the North Atlantic Treaty Organization (NATO) Workshop IST-153, ARL-SR-0396," April 2018. [Online]. Available: http://www.arl.army.mil/arlreports/2018/ARL-SR-0396.pdf.

[10] D. Bodeau, R. Graubart, L. LaPadula, P. Kertzner, A. Rosenthal and J. Brennan, "Cyber Resiliency Metrics," April 2012. [Online]. Available: https://registerdev1.mitre.org/sr/12_2226.pdf.

[11] D. Bodeau, R. Graubart, R. McQuaid and J. Woodill, "Cyber Resiliency Metrics Catalog," The MITRE Corporation, Bedford, MA, 2018.

[12] D. Bodeau, R. Graubart, R. McQuaid and J. Woodill, "Cyber Resiliency Metrics and Scoring in Practice: Use Case Methodology and Examples," The MITRE Corporation, Bedford, MA, 2018.

[13] D. Bodeau and R. Graubart, "Structured Cyber Resiliency Analysis Methodology (SCRAM) (PR Case No. 16-0777)," May 2016. [Online]. Available: https://www.mitre.org/publications/technical-papers/structured-cyber-resiliency-analysis-methodology.

[14] DoD, "DoD Dictionary of Military and Associated Terms," April 2018. [Online]. Available: http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/dictionary.pdf?ver=2018-05-02-174746-340.

[15] Defense Acquisition University, "Measure of Effectiveness (MOE)," Glossary of Defense Acquisition Acronyms and Terms, [Online]. Available: https://dap.dau.mil/glossary/pages/2236.aspx.

[16] D. Bodeau, R. Graubart and W. Heinbockel, "Mapping the Cyber Terrain: Enabling Cyber Defensibility Claims and Hypotheses to Be Stated and Evaluated with Greater Rigor and Utility (MTR130433)," 2013.

[Online]. Available: http://www.mitre.org/sites/default/files/publications/mapping-cyber-terrain-13-4175.pdf.

[17] R. Ford, M. Cavalho, L. Mayron and M. Bishop, "Toward Metrics for Cyber Resilience," in *21st EICAR (European Institute for Computer Anti-Virus Research) Annual Conference Proceedings*, 2012.

[18] NIST, "2nd Public Draft, NIST SP 800-160, Systems Security Engineering: Considerations for a Multidisciplinary Approach in the Engineering of Trustworthy Secure Systems," 4 May 2016. [Online]. Available: http://csrc.nist.gov/publications/drafts/800-160/sp800_160_second-draft.pdf.

[19] A. A. Ganin, E. Massaro, A. Gutfraind, N. Steen, J. M. Keisler, A. Kott, R. Mangoubi and I. Linkov, "Operational resilience: concepts, design, and analysis," *Nature: Scientific Reports,* vol. 6, no. 19540, 2016.

[20] G. Cybenko, "Quantifying and measuring cyber resiliency," in *Sensors, and Command, Control, Communications, and Intelligence (C3I) Technologies for Homeland Security, Defense, and Law Enforcement Applications XV, Proc. of SPIE Vol. 9825, 98250R*, Baltimore, MD, 2016.

[21] Z. A. Collier, M. Panwar, A. A. Ganin, A. Kott and I. Linkov, "Security Metrics in Industrial Control Systems," in *Cyber Security of Industrial Control Systems, Including SCADA Systems*, Springer, 2016, pp. 167-185.

[22] S. Musman and S. Agbolosu-Amison, "A Measurable Definition of Resiliency Using "Mission Risk" as a Metric," March 2014. [Online]. Available: http://www.mitre.org/sites/default/files/publications/resiliency-mission-risk-14-0500.pdf.

[23] P. Ramuhalli, M. Halappanavar, J. Coble and M. Dixit, "Towards A Theory of Autonomous Reconstitution of Compromised Cyber-Systems," *Homeland Security Affairs, Supplement 6,* p. April, 2014.

[24] World Economic Forum, "Partnering for Cyber Resilience: Toward the Quantification of Cyber Risks," 19 January 2015. [Online]. Available: http://www3.weforum.org/docs/WEFUSA_QuantificationofCyberThreats_Report2015.pdf.

[25] J. Park, T. P. Seager, P. S. Rao, M. Convertino and I. Linkov, "Integrating risk and resilience approaches to catastrophe management in engineering systems," *Risk Analysis,* vol. 33, no. 3, pp. 356-367, 2013.

[26] I. Linkov, D. A. Eisenberg, M. E. Bates, D. Chang, M. Convertino, J. H. Allen, S. E. Flynn and T. P. Seager, "Measurable Resilience for Actionable Policy," *Environmental Science & Technology,* vol. 47, p. 10108−10110, 2013.

[27] NIST, "NIST SP 800-30 Rev.1, Guide for Conducting Risk Assessments," September 2012. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

[28] Y. Cheng, J. Deng, J. Li, S. A. DeLoach, A. Singhal and X. Ou, "Metrics of Security," in *Cyber Defense and Situational Awareness, Advances in Information Security 62*, Springer International Publishing, 2014, pp. 263-265.

[29] S. Musman and A. Temin, "A Cyber Mission Impact Assessment Tool (PR 14-3545)," in *2015 IEEE International Symposium on Technologies for Homeland Security (HST)*, Waltham, MA, 2015.

[30] S. Noel, J. Ludwig, P. Jain, D. Johnson, R. K. Thomas, J. McFarland, B. King, S. Webster and B. Tello, "Analyzing Mission Impacts of Cyber Actions (AMICA), STO-MP-AVT-211," 1 June 2015. [Online]. Available: http://csis.gmu.edu/noel/pubs/2015_AMICA.pdf.

[31] H. Cam and P. Mouallem, "Mission-Aware Time-Dependent Cyber Asset Criticality and Resilience," in *Proceedings of the 8th CSIIRW Cyber Security and Information Intelligence Research Workshop*, Oak Ridge National Lab, Oak Ridge, TN, 2013.

[32] R. Sharman, R. Rao and S. Upadhyaya, "Metrics for Information Security - A literature survey," in *Proceedings of the 2004 Americas Conference on Information Systems (AMCIS)*, 2004.

[33] G. O. Yee, "Security Metrics: An Introduction and Literature Review," in *Computer and Information Security Handbook (Second Edition)*, Elsevier, 2013, pp. 57-70.

[34] ACSA, "Proceedings of the Workshop on Information Security System Scoring and Ranking (WISSR)," 21-23 May 2001. [Online]. Available: https://www.acsac.org/measurement/proceedings/wisssr1-proceedings.pdf.

[35] INFOSEC Research Council (IRC), "Hard Problems List," November 2005. [Online]. Available: http://www.infosec-research.org/docs_public/20051130-IRC-HPL-FINAL.pdf.

[36] DHS, "A Roadmap for Cybersecurity Research," November 2009. [Online]. Available: http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf.

[37] L. I. Millett, B. Fischhoff and P. J. Weinberger, "Foundational Cybersecurity Research: Improving Science, Engineering, and Institutions," 26 January 2017. [Online]. Available: https://www.nap.edu/download/24676.

[38] DHS, "FY 2017 CIO FISMA Metrics, Version 1.0," 1 October 2016. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/FY%202017%20CIO%20FISMA%20Metrics-%20508%20Compliant.pdf.

[39] Center for Internet Security, "The CIS Security Metrics, v1.1.0," 1 November 2010. [Online]. Available: https://downloads.cisecurity.org/compatibility.

[40] Dimensional Research, "2017 Trends in Security Metrics and Security Assurance Measurement Report: A Survey of IT Security Professionals," 30 March 2017. [Online]. Available: https://www.infosecurityeurope.com/__novadocuments/351566?v=636276211247070000.

[41] Cisco, "Unified Security Metrics: Vulnerability Metrics," 16 June 2016. [Online]. Available: https://www.cisco.com/c/dam/en/us/products/collateral/security/unified-security-metrics-framework.pdf.

[42] C. Alberts, J. Allen and R. Stoddard, "Risk-Based Measurement and Analysis: Application to Software Security, CMU/SEI-2012-TN-004," February 2012. [Online]. Available: https://resources.sei.cmu.edu/asset_files/TechnicalNote/2012_004_001_15428.pdf.

[43] World Economic Forum, "Partnering for Cyber Resilience: Risk and Responsibilities in a Hyperconnected World - Principles and Guidelines," March 2012. [Online]. Available: http://www3.weforum.org/docs/WEF_IT_PartneringCyberResilience_Guidelines_2012.pdf.

[44] Ponemon Institute, "The Third Annual Study on the Cyber Resilient Organization," 12 March 2018. [Online]. Available: https://info.resilientsystems.com/hubfs/IBM_Resilient_Branded_Content/White_Papers/2018_Cyber_Resilient_Organization_Study.pdf.

[45] SRP, "Library of Cyber Resilience Metrics," 16 January 2018. [Online]. Available: https://www.betaalvereniging.nl/wp-content/uploads/Library-of-Cyber-Resilience-Metrics-Shared-Research-Program-Cybersecurity.pdf.

[46] J. D. Peláez, "46 metrics to improve cyber resilience in an essential service," CERTSI, 23 November 2017. [Online]. Available: https://www.certsi.es/en/blog/46-metrics-improve-cyber-resilience-essential-service.

[47] CRO Forum, "Cyber resilience: The cyber risk challenge and the role of insurance," December 2014. [Online]. Available: http://www.thecroforum.org/wp-content/uploads/2014/12/Cyber-Risk-Paper-version-24.pdf.

[48] Cisco, "Cyber Risk and Resilience for Boards," 10 April 2018. [Online]. Available: https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cyber-risk-for-the-board.pdf.

[49] J. S. Brtis, "How to Think About Resilience in a DoD Context: A MITRE Recommendation (MTR 160138, PR 16-2051)," The MITRE Corporation, Colorado Springs, CO, 2016.

[50] O. Madaya, The Resilience of Networked Infrastructure Systems: Analysis and Measurement (Systems Research Series — Vol. 3), Hackensack, NJ: World Scientific Publishing Company, 2013.

[51] D. G. Dessavre and J. E. Ramirez-Marquez, "Computational Techniques for the Approximation of Total System Resilience," in *Safety and Reliability of Complex Engineered Systems: ESREL 2015*, Zurich, Switzerland, 2015.

[52] L. Wang, S. Jajodia, A. Singhal and S. Noel, "k-Zero Day Safety: Measuring the Security Risk of Networks against Unknown Attacks," in *European Symposium on Research in Computer Security (ESORICS)*, Athens, Greece, 2010.

[53] S. Noel and S. Jajodia, "Metrics Suite for Network Attack Graph Analytics," in *9th Annual Cyber and Information Security Research Conference (CISRC)*, Oak Ridge National Laboratory, TN, 2014.

[54] S. Noel, S. Jajodia, L. Wang and A. Singhal, "Measuring Security Risk of Networks Using Attack Graphs," *International Journal of Next-Generation Computing*, vol. 1, no. 1, 2010.

[55] S. Hassell, R. Case, G. Ganga, S. R. Martin, S. Marra and C. Eck, "Using DoDAF and Metrics for Evaluation of the Resilience of Systems, Systems of Systems, and Networks Against Cyber Threats," *INCOSE Insight*, pp. 26-28, April 2015.

[56] P. Beraud, A. Cruz, S. Hassell and S. Meadows, "Using Cyber Maneuver to Improve Network Resiliency," in *MILCOM*, Baltimore, MD, 2011.

[57] S. Martin and S. Hassell, "Cyber Analysis Evaluation Modeling for Operations - Countering the Cyberthreat," 2013. [Online]. Available: Cyber Analysis Modeling Evaluation for Operations (CAMEO) — Countering the Cyberthreat - See more at: http://www.raytheon.com/newsroom/technology_today/2013_i1/cameo.html#sthash.gYtx3MKS.dpuf.

[58] S. Musman and A. Turner, "A game theoretic approach to cyber security risk management," *The Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, 2017.

[59] G. C. Bowker and S. L. Star, Sorting Things Out: Classification and Its Consequences, The MIT Press, 1999.

[60] M. Albanese, S. Jajodia and S. Noel, "Time-Efficient and Cost-Effective Network Hardening Using Attack Graphs," in *42nd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Boston, MA, 2012.

[61] NIST, "NIST SP 800-193, Platform Firmware Resiliency Guidelines," May 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-193.pdf.

[62] M. Aziz-Alaoui, C. Bertelle and (eds.), From System Complexity to Emergent Properties, Springer, 2009.

[63] N. Husted and S. Myers, "Emergent Properties & Security: The Complexity of Security as a Science," in *New Security Paradigms Workshop (NSPW'14)*, Victoria, British Columbia, 2014.

[64] A. A. Ganin, E. Massaro, A. Gutfraind, N. Steen, J. M. Keisler, A. Kott, R. Mangoubi and I. Linkov, "Operational resilience: concepts, design and analysis," Nature.com Scientific Reports, 19 January 2016. [Online]. Available: http://www.nature.com/articles/srep19540.

[65] Z. A. Collier, I. Linkov and J. H. Lambert, "Four domains of cybersecurity: a risk-based systems approach to cyber decisions," *Environmental Systems & Decisions*, vol. 33, no. 4, pp. 469-470, 2013.

[66] I. Linkov, D. A. Eisenberg, K. Plourde, T. P. Seager, J. Allen and A. Kott, "Resilience metrics for cyber systems," *Environment Systems & Decisions*, vol. 33, no. 4, pp. 471-476, 2013.

[67] Z. A. Collier and I. Linkov, "Decision Making for Resilience within the Context of Network Centric Operations," in *19th Annual International Command and Control Research and Technology Symposium (19th ICCRTS)*, Alexandria, VA, 2014.

[68] Z. A. Collier, M. Panwar, A. A. Ganin, A. Kott and I. Linkov, "Security Metrics in Industrial Control Systems," in *Cyber Security of Industrial Control Systems, Including SCADA Systems; Advances in Information Security, Volume 66*, Springer, 2016.

[69] B. Keys, A. Chhajer, Z. Liu, D. Horner and S. Shapiro, "A Framework for Assessing Cyber Resilience: A Report for the World Economic Forum," 28 April 2016. [Online]. Available: http://bloustein.rutgers.edu/wp-content/uploads/2016/05/2016_WEF.pdf.

[70] D. Cross, "Rigor and Reproducibility in Federally-Funded Scientific Research: What are the Right Questions to Ask?," 3 November 2017. [Online]. Available: https://clarivate.com/wp-content/uploads/2017/11/nov-update_Rigor_and_Reproducibility_Whitepaper_SAR_17.pdf.

[71] I. Linkov, C. Fox-Lent, C. R. Allen, J. C. Arnott, E. Bellini, J. Coaffee, M.-V. Florin, K. Hatfield, I. Hyde, W. Hynes, A. Jovanovic, R. Kasperson, J. Katzenberger, P. W. Keys, J. H. Lambert, R. Moss, P. S. Murdoch, J. Polma-Oliveira, R. S. Pulwart, L. Read, D. Sands, E. A. Thomas, M. R. Tye and D. Woods, "Tiered Approach to Resilience Assessment," *Risk Analysis*, 2018.

[72] J.-P. Watson, R. Guttromson, C. Silva-Monroy, R. Jeffers, K. Jones, J. Ellison, C. Rath, J. Gearhart, D. Jones, T. Corbet, C. Hanley and L. T. Walker, "Conceptual Framework for Developing Resilience Metrics for US Electricity, Oil, and Gas Sectors, SAND2014-18019," September 2015. [Online]. Available: http://energy.gov/sites/prod/files/2015/09/f26/EnergyResilienceReport_%28Final%29_SAND2015-18019.pdf.

[73] NIST, "NIST SP 800-53 R4, Security and Privacy Controls for Federal Information Systems and Organizations," April 2013. [Online]. Available: http://dx.doi.org/10.6028/NIST.SP.800-53r4.

[74] NIST, "Framework for Improving Critical Infrastructure Security, Version 1.0," 12 February 2014. [Online]. Available: http://www.nist.gov/cyberframework/upload/cybersecurity-framework-021214.pdf.

[75] NIST, "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," 16 April 2018. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[76] D. Bodeau and R. Graubart, "Characterizing Effects on the Cyber Adversary: A Vocabulary for Analysis and Assessment (MTR 130432, PR 13-4173)," November 2013. [Online]. Available: http://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf.

[77] N. Ricci, D. H. Rhodes and A. M. Ross, "Evolvability-Related Options in Military Systems of Systems," in *Conference on Systems Engineering Research (CSER 2014)*, Redondo Beach, CA, 2014.

[78] NIST, "NIST SP 800-55R1, Performance Measurement Guide for Information Security," July 2008. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-55r1.pdf.

[79] IATAC, "Measuring Cyber Security and Information Assurance: State-of-the-Art Report (SOAR)," 8 May 2009. [Online]. Available: https://www.csiac.org/csiac-report/measuring-cyber-security-and-information-assurance/.

[80] J. Allen and N. Davis, "Measuring Operational Resilience Using the CERT® Resilience Management Model," September 2010. [Online]. Available: http://www.cert.org/archive/pdf/10tn030.pdf.

[81] The MITRE Corporation, "Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™)," The MITRE Corporation, 2015. [Online]. Available: https://attack.mitre.org/wiki/Main_Page.

[82] ODNI, "Cyber Threat Framework," [Online]. Available: https://www.dni.gov/index.php/cyber-threat-framework.

[83] National Security Agency, "NSA/CSS Technical Cyber Threat Framework v1," 6 March 2018. [Online]. Available: https://www.iad.gov//iad/library/reports/assets/public/upload/NSA-CSS-Technical-Cyber-Threat-Framework-v1.pdf.

[84] D. Bodeau and R. Graubart, "Cyber Prep 2.0: Motivating Organizational Cyber Strategies in Terms of Preparedness (MTR 150264, PR 16-0939)," The MITRE Corporation, Bedford, MA, 2016.

[85] D. Bodeau and R. Graubart, "A Framework for Describing and Analyzing Cyber Strategies and Strategic Effects (MTR 140346, PR 14-3407)," The MITRE Corporation, Bedford, MA, 2014.

[86] D. J. Bodeau, C. D. McCollum and D. B. Fox, "Cyber Threat Modeling: Survey, Assessment, and Representative Framework (PR 18-1174)," The MITRE Corporation, McLean, VA, 2018.

[87] C. D. Doğan and M. Uluman, "Comparison of Rubrics and Graded Category Rating Scales with Various Methods Regarding Raters' Reliability," *Educational Sciences: Theory and Practice,* vol. 17, no. 2, pp. 631-651, 2017.

[88] H. Aguinis, S. A. Culpepper and C. A. Pierce, "Differential prediction generalization in college admissions testing," *Journal of Educational Psychology,* vol. 108, no. 7, pp. 1045-1059, 2016.

[89] K. Kirkpatrick, "Battling Algorithmic Bias," *Communications of the ACM,* pp. 16-17, October 2016.

[90] J. Pagels, "The Scoring For The Decathlon And Heptathlon Favors Running Over Throwing," FiveThirtyEight, 17 August 2016. [Online]. Available: https://fivethirtyeight.com/features/the-scoring-for-the-decathlon-and-heptathlon-favors-running-over-throwing/.

[91] M. Pilon, A. W. Lehren, S. Gosk, E. R. Siegel and K. Abou-Sabe, "Think Olympic figure skating judges are biased? The data says they might be.," NBC News, 6 February 2018. [Online]. Available: https://www.nbcnews.com/storyline/winter-olympics-2018/think-olympic-figure-skating-judges-are-biased-data-says-they-n844886.

[92] FICO, "FICO Enterprise Security Score: The Science of Cybersecurity Predictive Analytics," 1 June 2017. [Online]. Available: http://www.fico.com/en/node/8140?file=12697.

[93] M. Reed, S. Hanson and D. Schaffner, "How Cyber FICO Ratings Could Benefit Insurance Underwriting," Insurance Journal, 7 March 2018. [Online]. Available: https://www.insurancejournal.com/?p=482548.

[94] SecurityScorecard, "SecurityScorecard," 2018. [Online]. Available: https://securityscorecard.com/.

[95] BitSight, "BitSight Security Ratings," 5 June 2018. [Online]. Available: https://cdn2.hubspot.net/hub/277648/file-2505376057.pdf?__hssc=204656143.1.1529363212598&__hstc=204656143.89be6a63fbaa65c464930c3a9c4d1455.1529363212598.1529363212598.1529363212598.1&__hsfp=785420633&hsCtaTracking=f61c59d6-1e16-46df-b34d-bf4891e35bc1%7C06.

[96] FireCompass, "How Mature is Your Cyber Security?," 2018. [Online]. Available: https://www.firecompass.com/cyber-security-maturity-score/.

[97] NormShield, "NormShield Cyber Risk Scorecards," 2018. [Online]. Available: https://www.normshield.com/.

[98] A. Smith, "Office 365 Secure Score is now Microsoft Secure Score," Microsoft, 17 April 2018. [Online]. Available: https://techcommunity.microsoft.com/t5/Security-Privacy-and-Compliance/Office-365-Secure-Score-is-now-Microsoft-Secure-Score/ba-p/182358.

[99] Norton, "Norton Core Security Score," 3 August 2017. [Online]. Available: https://support.norton.com/sp/en/us/home/current/solutions/v118380521_core_en_us.

[100] Fortinet, Inc., "Security Fabric Score," 2018. [Online]. Available: http://help.fortinet.com/fos50hlp/56/Content/FortiOS/fortigate-security-fabric/Whats%20new%20content/5-score.htm.

[101] RiskSense, "RiskSense Unveils FICO®-Like Cyber Risk Scoring to Pinpoint Threats That Require Immediate Attention," 21 June 2016. [Online]. Available: https://www.risksense.com/news/press-releases/RiskSense-Unveils-FICO-Like-Cyber-Risk-Scoring-to-Pinpoint-Threats-That-Require-Immediate-Attention/.

[102] UpGuard, "Visualizing Cyber Risk with UpGuard's Home Page Dashboard," UpGuard, 31 May 2018. [Online]. Available: https://www.upguard.com/blog/upguards-home-page-dashboard.

[103] Synack, "A Security Score Built for Attacker Resistance," 17 April 2018. [Online]. Available: https://www.synack.com/2018/04/17/security-score-attacker-resistance/.

[104] EPRI, "Cyber Security Metrics for the Electric Sector," 1 September 2017. [Online]. Available: https://publicdownload.epri.com/PublicDownload.svc/product=000000003002011685/type=Product.

[105] FIRST.Org, Inc., "Common Vulnerability Scoring System v3.0: Specification Document," 2 August 2017. [Online]. Available: https://www.first.org/cvss/cvss-v30-specification-v1.8.pdf.

[106] R. Martin and S. Christey, "Common Weakness Scoring System (CWSS™)," 5 September 2014. [Online]. Available: https://cwe.mitre.org/cwss/cwss_v1.0.1.html.

[107] NCCIC, "National Cybersecurity and Communications Integration Center (NCCIC) Incident Scoring System," 23 March 2017. [Online]. Available: https://www.us-cert.gov/NCCIC-Cyber-Incident-Scoring-System.

[108] G. Roldán-Molina, M. Vitor Basto-Fer, C. Silva-Rabadão, I. Yevseyeva and V. Basto-Fernandes, "A Comparison of Cybersecurity Risk Analysis Tools," in *International Conference on Project MANagement / HCist - International Conference on Health and Social Care Information Systems and Technologies*, Barcelona, Spain, 2017.

[109] A. A. Ganin, P. Quach, M. Panwar, Z. A. Collier, J. M. Keisler, D. Marchese and I. Linkov, "Multicriteria Decision Framework for Cybersecurity Risk Analysis," *Risk Analysis*, no. September, 2017.

[110] The MITRE Corporation, "Systems Engineering Guide: Crown Jewels Analysis," 2011. [Online]. Available: http://www.mitre.org/publications/systems-engineering-guide/enterprise-engineering/systems-engineering-for-mission-assurance/crown-jewels-analysis.

[111] Y. Haimes, "Risk Modeling of Interdependent Complex Systems of Systems: Theory and Practice," *Risk Analysis*, vol. 38, no. 1, pp. 84-98, 2018.

[112] A. E. Schulz, M. C. Kotson and J. R. Zipkin, "Cyber Network Mission Dependencies, Technical Report 1189," 2015. [Online]. Available: https://www.ll.mit.edu/mission/cybersec/publications/publication-files/full_papers/2015-Schultz-TR-1189.pdf.

[113] S. Noel, E. Harley, K. H. Tam, M. Limiero and M. Share, "CyGraph: Graph-Based Analytics and Visualization for Cybersecurity," in *Cognitive Computing: Theory and Applications (Volume 35 of Handbook of Statistics)*, Elsevier, 2016.

[114] W. Bryant, "Cyber Resiliency: Springing Back with the Bamboo," in *Evolution of Cyber Technologies and Operations to 2035, Advances in Information Security Volume 63*, Springer International Publishing, 2015, pp. 1-17.

[115] INFOSEC Institute, "Getting Started with IoT Security - Mapping the Attack Surface," INFOSEC Institute, 18 May 2016. [Online]. Available: http://resources.infosecinstitute.com/getting-started-with-iot-security-mapping-the-attack-surface/#gref.

[116] P. K. Manadhata and J. M. Wing, "An Attack Surface Metric," *IEEE Transactions on Software,* vol. 37, no. 3, 2011.

[117] D. B. Fox, E. I. Arnoth, C. W. Skorpuka, C. D. McCollum and D. J. Bodeau, "Enhanced Cyber Threat Model for Financial Services Sector (FSS) Institutions: Threat Model ATT&CK/CAPEC Version (PR 18-1725)," The MITRE Corporation, McLean, VA, 2018.

[118] R. D. Graubart, E. Laderman and J. Snyder, "Beyond the Baselines: Identifying Environmental Assumptions for Security Controls," The MITRE Corporation, Bedford, MA, 2016.

[119] NIST, "NIST SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View," March 2011. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf.

[120] A. Temin and S. Musman, "A Language for Capturing Cyber Impact Effects, MTR 100344, PR 10-3793," The MITRE Corporation, Bedford, MA, 2010.

[121] CPS PWG, "Framework for Cyber-Physical Systems, Release 1.0," May 2016. [Online]. Available: https://s3.amazonaws.com/nist-sgcps/cpspwg/files/pwgglobal/CPS_PWG_Framework_for_Cyber_Physical_Systems_Release_1_0Final.pdf .

[122] NSF, "Cyber-Physical Systems: Enabling a Smart and Connected World," National Science Foundation, 2018. [Online]. Available: https://www.nsf.gov/news/special_reports/cyber-physical/.

[123] L. Wang, M. Törngren and M. Onori, "Current status and advancement of cyber-physical systems inmanufacturing," *Journal of Manufacturing Systems,* vol. 37, no. 517-527, 2015.

[124] CyPhERS Project, "Deliverable D2.2: Structuring of CPS Domain: Characteristics, trends, challenges, and opportunities associated with CPS," 28 May 2014. [Online]. Available: http://www.cyphers.eu/sites/default/files/D2.2.pdf.

[125] CPS PWG, "Framework for Cyber-Physical Systems: Volume 1, Overview, Version 1.0, NIST SP 1500-201," June 2017. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-201.pdf.

[126] NIST, "NIST SP 800-184, Guide for Cybersecurity Event Recovery," December 2016. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-184.pdf.

[127] NICCS, "NICCS Glossary," National Initiative for Cybersecurity Careers and Studies, 27 November 2017. [Online]. Available: https://niccs.us-cert.gov/glossary.

[128] CNSS, "Committe on National Security Systems (CNSS) Glossary (CNSS Instruction No. 4009)," 26 April 2015. [Online]. Available: https://www.cnss.gov/CNSS/openDoc.cfm?hldYMe6UHW4ISXb8GFGURw==.

[129] NIST, "Glossary of Key Information Security Terms, NISTIR 7298, Revision 2," May 2013. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf.

[130] DHS, "U. S. Department of Homeland Security Cybersecurity Strategy," 15 May 2018. [Online]. Available: https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf.

[131] ISO, "ISO/IEC TR 13066-4:2015, Information technology — Interoperability with assistive technology (AT) — Part 4: Linux/UNIX graphical environments accessibility API," ISO Online Browsing Platform, 2015. [Online]. Available: https://www.iso.org/obp/ui/#iso:std:iso-iec:tr:13066:-4:ed-1:v1:en.

[132] DAU, "Defense Acquisition Portal," Defense Acquisition University (DAU), [Online]. Available: https://dap.dau.mil/aphome/das/Pages/Default.aspx.

[133] NIST Big Data Public Working Group (NBD-PWG) Reference Architecture Subgroup, "NIST Big Data Interoperability Framework: Volume 6, Reference Architecture, Final Version 1, NIST Special Publication 1500-6," September 2015. [Online]. Available: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1500-6.pdf.

[134] C. Woody and C. Alberts, "Evaluating Security Risks Using Mission Threads," *CrossTalk,* pp. 15-19, September / October 2014.

[135] DON CIO, "Platform Information Technology Definitions for the Department of the Navy," 7 November 2007. [Online]. Available: http://www.doncio.navy.mil/uploads/Enclosure1_PlatformITDefinitionsforDON%5B2%5D.pdf.

[136] DoD, "DoD Program Manager's Guidebook for Integrating the Cybersecurity Risk Management Framework (RMF) into the System Acquisition Lifecycle, Version 1.0," 26 May 2015. [Online]. Available: https://acc.dau.mil/adl/en-US/722603/file/80119/Cybersecurity%20Guidebook%20v1_0%20with%20publication%20notice.pdf.

[137] DoD CIO, "DoDI 8500.01, Cybersecurity," 14 March 2014. [Online]. Available: http://www.dtic.mil/whs/directives/corres/pdf/850001_2014.pdf.

[138] NIST, "NIST SP 800-66 Rev. 1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA)," October 2008. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-66r1.pdf.

[139] ISO/IEC JTC 1/SC 7, ISO/IEC/IEEE 15288:2015 - Systems and software engineering -- System life cycle processes, Geneva, Switzerland: International Standards Organization, 2015.

[140] C. Zimmerman, Ten Strategies of a World-Class Computer Security Incident Response Team, Mclean,VA: The MITRE Corporation, 2014.

[141] R. van Solingen and E. Berghout, The Goal/Question/Metric Method: a practical guide for quality improvement of software development, London: McGraw-Hill, 1999.

[142] LeMay Center for Doctrine, Air University, "Assessment Measures," Annex 3.0 - Operations & Planning, 4 November 2016. [Online]. Available: https://doctrine.af.mil/download.jsp?filename=3-0-D27-OPS-Assessment-Measure.pdf.

[143] S. Shetty, B. Krishnappa and D. Nichol, "Cyber Resilience Metrics for Bulk Power Systems," Industrial Control Systems Joint Working Group (ICSJWG) Quarterly Newsletter, March 2017. [Online]. Available: https://cred-c.org/sites/default/files/papers/2017_Q1_CRMetricsBPS_Published.pdf.

[144] D. A. Eisenberg, I. Linkov, J. Park, M. E. Bates, C. Fox-Lent and T. P. Seager, "Resilience Metrics: Lessons from Military Doctrines," *Solutions,* vol. 5, no. 5, pp. 76-85, September 2014.

[145] A. M. Madni and S. Jackson, "Towards a Conceptual Framework for Resilience Engineering," *IEEE Systems Journal, Vol. 3, No. 2,* June 2009.

[146] The MITRE Corporation, "The MITRE Cyber Resiliency FAQ, PR 17-1434," 15 May 2017. [Online]. Available: https://www.mitre.org/sites/default/files/PR_17-1434.pdf.

[147] Z. A. Collier, M. Panwar, A. A. Ganin, A. Kott and I. Linkov, "Security Metrics in Industrial Control Systems," in *Cyber Security of Industrial Control Systems, Including SCADA Systems*, New York, NY, Springer, 2016.

[148] IEEE Computer Society, "Enterprise IT Body of Knowledge - Glossary," Enterprise IT Body of Knowledge , 23 March 2017. [Online]. Available: http://eitbokwiki.org/Glossary#eit.

[149] NIST, "Enterprise Architecture (EA)," Computer Security Resource Center (CSRC) Glossary, 2017. [Online]. Available: https://csrc.nist.gov/Glossary/?term=1522.

[150] M. Wetzler, "Architecture of Giants: Data Stacks at Facebook, Netflix, Airbnb, and Pinterest," Keen IO, 4 April 2017. [Online]. Available: https://blog.keen.io/architecture-of-giants-data-stacks-at-facebook-netflix-airbnb-and-pinterest-9b7cd881af54.

[151] I. Gasparetto, "Developing applications for Big Data," Techifide, 27 April 2017. [Online]. Available: https://www.techifide.com/big-data-technology-development/.

[152] Office of the DASD (DT&E), "Guidelines for Cybersecurity DT&E, version 1.0," 19 April 2013. [Online]. Available: https://acc.dau.mil/adl/en-US/649632/file/71914/Guidelines%20for%20Cybersecurity%20DTE%20v1.0%2020130419.pdf.

[153] D. J. Zelik, E. S. Patterson and D. D. Woods, "Measuring attributes of rigor in information analysis," in *Macrorecognition Metrics and Scenarios: Design and Evaluation for Real-World Teams,* Aldershot, UK, Ashgate, 2010.

[154] R. A. Caralli, J. H. Allen, D. W. White, L. R. Young, N. Mehravari and P. D. Curtis, "CERT® Resilience Management Model, Version 1.2," February 2016. [Online]. Available: http://www.cert.org/downloads/resilience/assets/cert-rmm-v1-2.pdf.

[155] J. Zalewski, I. A. Buckley, B. Czejdo, S. Drager, A. J. Kornecki and N. Subramanian, "A Framework for Measuring Security as a System Property in Cyberphysical Systems," *Information,* vol. 7, no. 33, 2016.

[156] A. Lacher, "Autonomy & Transportation: Addressing Cyber-Resiliency Challenges, PR 15-1841," 10 June 2015. [Online]. Available: http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2015-06/ispab_june-10_alacher.pdf.

[157] NIST, "NIST SP 800-34 Rev. 1, Contingency Planning Guide for Federal Information Systems," 11 November 2010. [Online]. Available: http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf. [Accessed 19 May 2011].

[158] C. C. Demchak, "Resilience and Cyberspace: Recognizing the Challenges of a Global Socio-Cyber Infrastructure (GSCI)," *Journal of Comparative Policy Analysis: Research and Practice,* vol. 143, no. 3, pp. 254-269, 2012.

[159] S. Hosseini, K. Barker and J. E. Ramirez-Marquez, "A review of definitions and measures of system resilience," *Reliability Engineering and System Safety,* vol. 145, pp. 47-61, 2016.

[160] DHS, "Cyber Resilience White Paper: An Information Technology Sector Perspective," March 2017. [Online]. Available: http://www.it-scc.org/uploads/4/7/2/3/47232717/it_sector_cyber_resilience_white_paper.pdf.

Appendix A Cyber Resiliency Constructs, Metrics, and MOEs

This Appendix describes the relationships between cyber resiliency constructs, constructs describing the operational environment, and cyber resiliency metrics for systems, missions, and programs. The constructs to which a cyber resiliency metric is designed to relate strongly influence its form, fidelity, and generality. The constructs to which a given metric or MOE are related can be characterized by the stakeholders whose questions the metric is intended to answer, as illustrated notionally in Figure 14. These four perspectives – program management, systems engineering, mission assurance, and threat – motivate the definition of metrics with varying degrees of rigor and granularity. The relationship between metrics and constructs clarifies relationships between different types of metrics, thereby providing a foundation for "roll-up rules" – algorithms or processes for using the values of some metrics as inputs to others.

Figure 14. Different Stakeholders Seek Metrics to Answer Different Questions

A.1 Cyber Resiliency Constructs and Perspectives on a System

Figure 15 illustrates how the constructs reflect two different perspectives on a system. From a program management perspective, cyber resiliency goals and objectives express desired system properties. The relative priorities of goal will drive the relative priorities of objectives, as indicated by the dashed line. From a systems engineering perspective, cyber resiliency design principles and techniques inform the definition of cyber resiliency solutions; a given solution can apply cyber resiliency design principles and techniques. (As will be discussed in the next section, cyber resiliency goals and solutions are situated in and provide links to additional contexts.) Note that cyber resiliency design principles are shown at the interface between the program management and systems engineering perspectives; this illustrates how design principles serve as succinct expressions of analytic and design approaches, to facilitate shared understanding between the two perspectives.

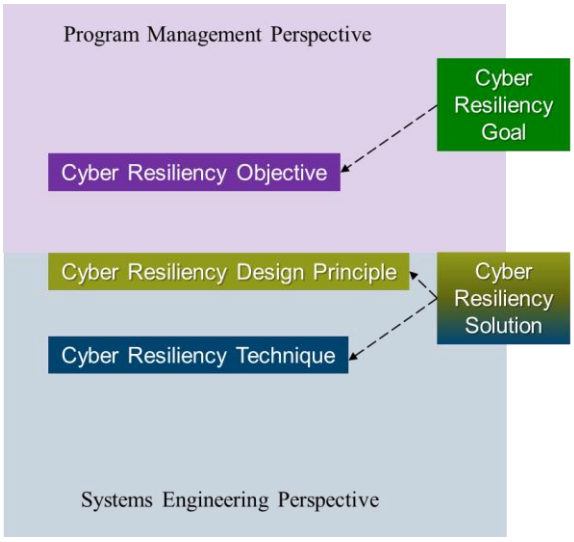

Figure 15. Perspectives on CREF Constructs

Figure 16 illustrates high-level or generic assessments (in *italics*) related to these constructs, using qualitative or semi-quantitative scales and evaluated using subject matter expert (SME) judgment. Dashed lines indicate metrics for a construct. For a cyber resiliency objective, assessments are of relative priority and how well the objective is achieved. For a cyber resiliency design principle or a cyber resiliency technique, assessments are of relevance, how broadly the design principle or technique is applied, and how well it is applied. For an approach to implementing a cyber resiliency technique, assessments are of relevance and of how well it is applied; most cyber resiliency approaches will be applied in targeted ways rather than broadly.

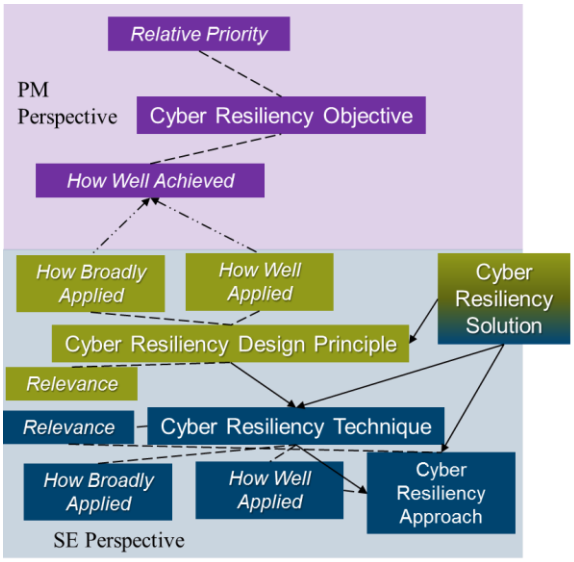

Figure 16. High-Level or Generic Assessments Related to CREF Constructs

Dot-dashed lines indicate that, because cyber resiliency design principles relate strongly to cyber resiliency objectives, how well and how broadly a design principle is applied can be considered in the assessment of how well an objective is achieved. Solid lines indicate other relationships between constructs: a cyber resiliency design principle indicates whether and how a cyber resiliency technique should be used; a cyber resiliency technique can be implemented using a variety of approaches; and a cyber resiliency solution can apply a cyber resiliency design principle, technique, and approach.

A.2 Assessing Cyber Resiliency Properties

Cyber resiliency *properties* are (or are directly related to) "how well" statements, expressing how well a system achieves cyber resiliency objectives and, to a lesser extent, how well a system architecture or design applies a cyber resiliency design principle or technique. For example, system robustness relates to how well the system achieves the Prevent / Avoid and Continue objectives. As indicated in the discussion of Figure 17, "how well" can be evaluated directly by SME judgment. However, additional constructs can be used to capture a more nuanced rationale for assessments of cyber resiliency properties.

Figure 18 illustrates how, for a given system or type of system, additional constructs can be defined for the program management perspective: sub-objectives and activities. These are discussed in more detail in Sections 2.2 and 3.1, with representative sub-objectives and activities identified in Appendix B. As discussed in Section 5.2, objectives, sub-objectives, and activities can be assigned a relative priority. For each activity, an assessment of how well it is (or could be) performed can be made; these can be rolled up into assessments of how well sub-objectives and ultimately objectives are achieved. The assessment of how well an activity is performed takes into consideration how – and how well – the cyber resiliency techniques and approaches which support it have been applied. As Figure 18 illustrates, the relative priority of an activity helps determine the relevance of cyber resiliency techniques and approaches.[23]

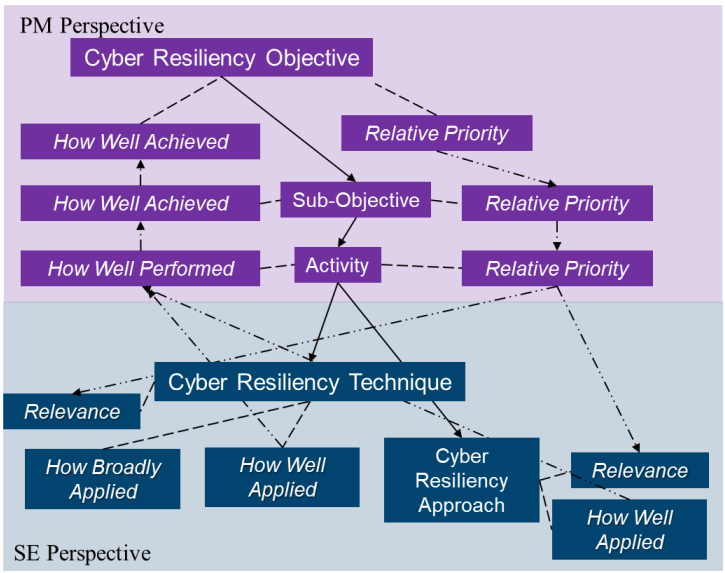

Figure 17. Relationships Among Assessments of More Granular Cyber Resiliency Constructs

Figure 18 provides an example of such relationships, showing how the relative priority of the Constrain objective, its sub-objective "Minimize degradation of service delivery," and one of the representative activities determine the relevance of the Dynamic Reconfiguration approach to implementing the Adaptive Response technique. The assessment of how well the approach is applied supports the assessment of how well Adaptive Response is applied. This supports the assessment of how well the representative activity is or can be performed, and hence how well the sub-objective and ultimately the objective are achieved. A quantitative metric (e.g., percentage of cyber resources which can be reconfigured on demand) can provide evidence for how well the approach is applied and how well the activity can be performed, as well as how well the "Change or disrupt the attack surface " design principle is applied.

[23] In addition, (and as discussed in Section 2.2, just as the relative priorities of objectives, sub-objectives, and activities depend on some aspects of the system context (e.g., mission, operational concept, threat environment), the relevance of cyber resiliency techniques and approaches depends on other aspects (e.g., system architecture, legacy technology investments).

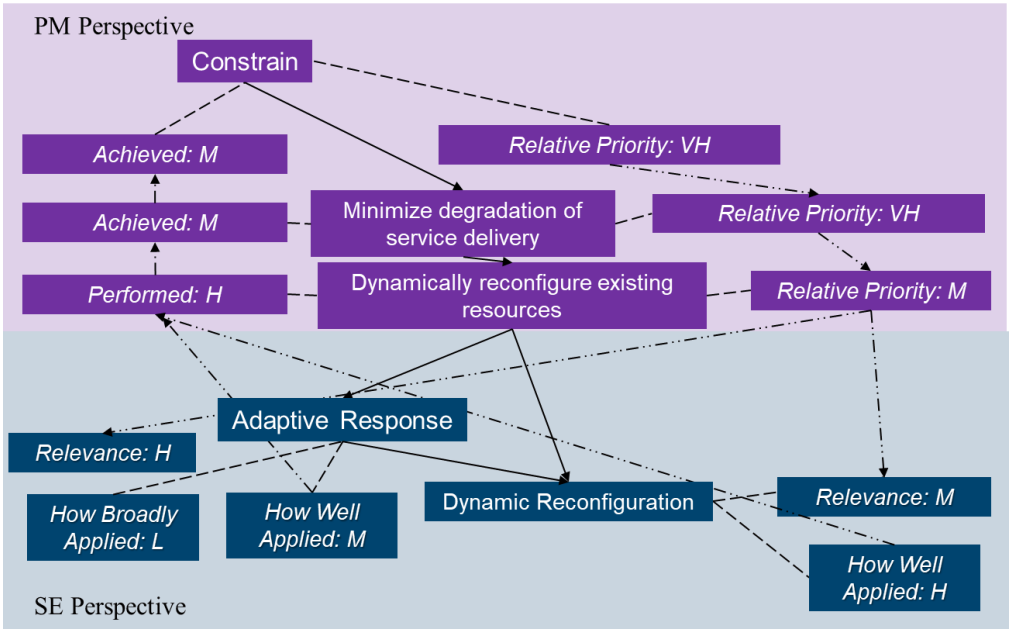

Figure 18. Example of Relationships Among Assessments Related to the Constrain Objective

For a given system, program, or use case, sub-objectives and activities should be grounded in the mission context – that is, they should be stated in terms of primary or supporting missions and mission activities, and relative priorities assigned based on how they support mission objectives.

As Figure 18 illustrates, representative activities provide a link to the systems engineering view: they are supported by cyber resiliency techniques and approaches, and often can be translated into functional requirements. Thus, the relative priorities of a sub-objective and of the activities which support it determine, in part, the relevance of cyber resiliency techniques and approaches. How well cyber resiliency techniques and approaches are applied, in turn, determine how well an activity is performed, and thus how well a sub-objective is achieved, and ultimately how well an objective is achieved.[24] These relationships support the definition of "roll-up rules" – more accurately, given that assessments of "how well" are qualitative or semi-quantitative and reflect SME judgment, these relationships support the definition of analytic processes for using the results of assessments of how well approaches and techniques are applied as inputs to assessments of how well activities are performed, and ultimately of how well objectives are achieved. As will be discussed below, cyber resiliency metrics can be defined that serve as indicators of, surrogates for, or inputs to assessments of "how well."

In addition to SME assessments, quantitative *performance metrics* can be defined for representative activities. For example, for the "Use shared threat information" activity mentioned above, representative metrics include the number of threat information feeds the organization uses, the frequency with which the organization's or a facility's local threat information database is updated, the time between the receipt of threat intelligence and a determination of its relevance, and the time between the determination that threat intelligence is relevant and the promulgation of defensive tactics, techniques, and procedures (TTPs).

[24] Assessments of "how well" can be made not only for an "as-is" system, but also for potential systems (e.g., alternative architectures, proposed changes to an implementation, proposed changes to operational processes).

A.3 Environmental Constructs

The environment in which a system operates and cyber resiliency is sought has multiple aspects, including mission, operations, governance, technology, and threat. For purposes of discussing metrics, the environment can be viewed from the mission assurance and threat perspectives as illustrated in Figure 19. From a mission assurance perspective, mission objectives are paramount. These objectives must be achieved in the intended operational context, and in the presence of threats. Thus, a characterization of the mission environment includes a threat model. As Figure 19 illustrates, cyber resiliency goals (or the corresponding resilience goals) can be viewed from a mission assurance as well as a Program Management perspective, providing a bridge between these two views of the problem domain. A cyber resiliency solution can be viewed from any of the four perspectives.

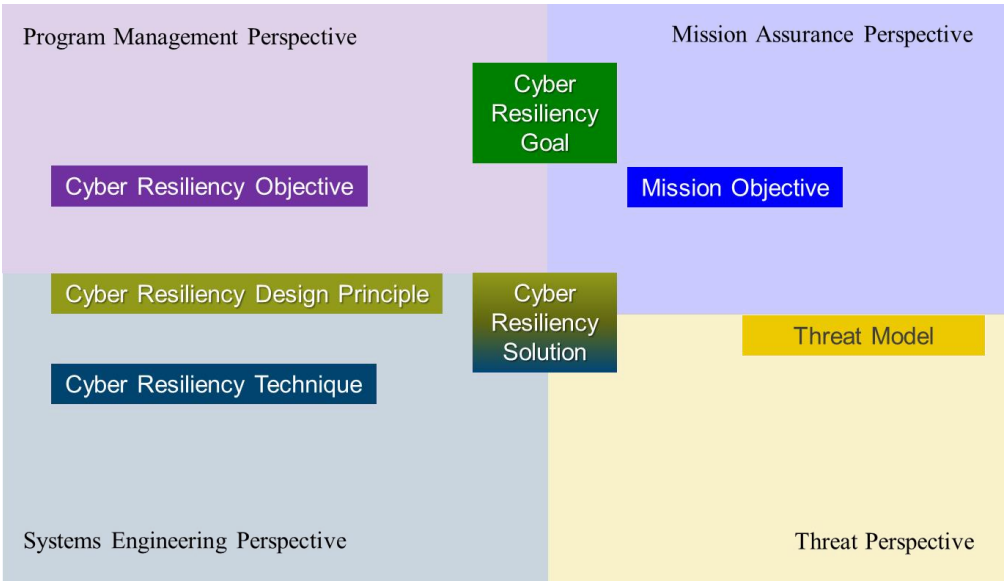

Figure 19. Adding the Mission Assurance and Threat Perspectives

Figure 20 illustrates how the mission assurance perspective informs cyber resiliency priorities, and how assessments of cyber resiliency properties can inform assessments of mission measures of performance (MOPs). Mission objectives, like cyber resiliency goals and objectives, have different relative priorities, and are achieved to a greater or lesser extent.[25] The relative priorities of different mission objectives inform the relative priorities of cyber resiliency goals and objectives. How well a mission objective is achieved can be assessed directly though qualitatively, by subject matter experts SMEs. Alternately, or as evidence in support of a qualitative assessment, a mission MOE or MOP can be used.[26]

Figure 21 provides an example of how an assessment of a cyber resiliency objective relates to a mission MOP. In the example, the mission objective is to deliver correct location data. The relative priority of this mission objective determines the relative priority of the Withstand goal and the Continue objective. The assessment of how well the Continue objective is achieved relates to the mission MOP for timely delivery of correct data. Both the SME assessment of the cyber resiliency objective and the quantitative evaluation of the MOP are made under the assumption of adverse conditions, i.e., with reference to the threat model.

[25] Note that "mission objectives" can be construed narrowly, in terms of the primary mission the system is intended to support, or can be construed broadly, to include supporting missions. Cybersecurity can be an important supporting mission, with objectives of confidentiality, integrity, and availability, as can cyber defense, with objectives of protect, detect, and react, or identify, protect, detect, respond, and recover.

[26] A *measure of effectiveness* is a "criterion used to assess changes in system behavior, capability, or operational environment that is tied to measuring the attainment of an end state, achievement of an objective, or creation of an effect." [142]

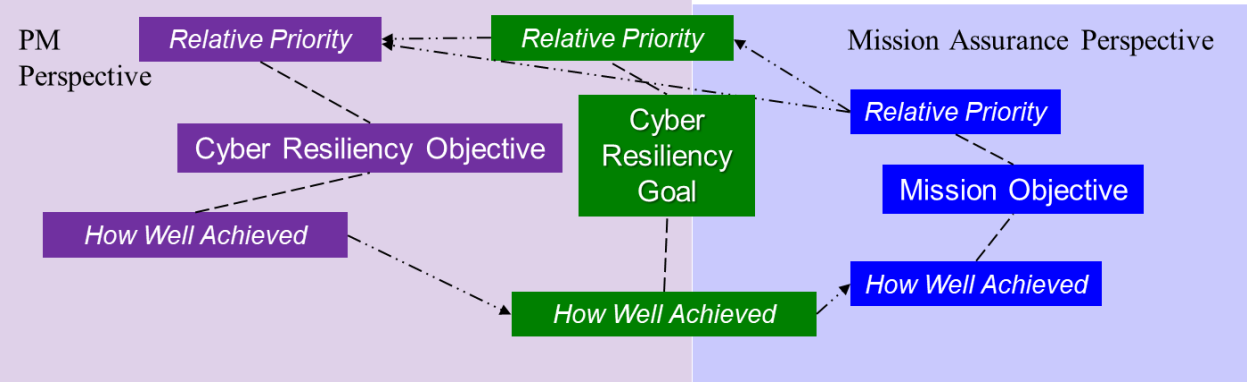

Figure 20. Mission Priorities Inform Cyber Resiliency Priorities

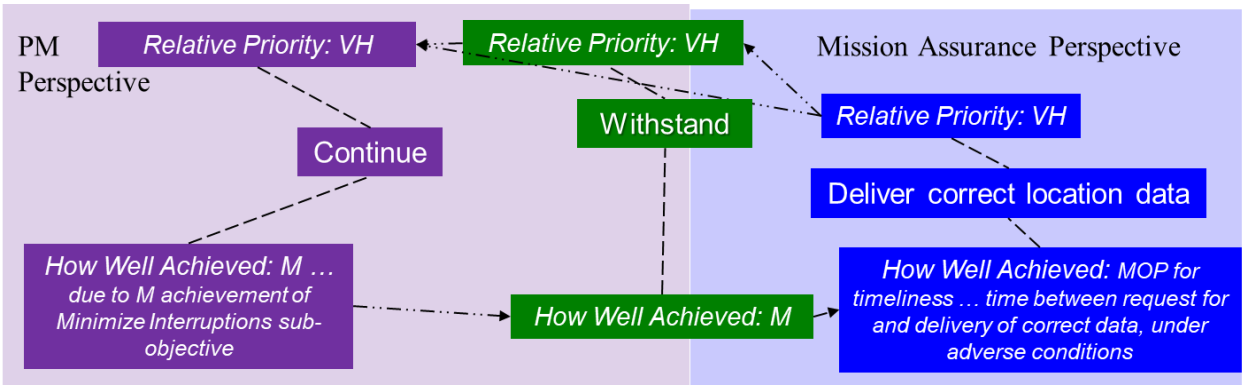

Figure 21. Relationship Between Cyber Resiliency Assessment and Mission Measures of Performance

Figure 22 illustrates the relationship between cyber resiliency properties and the threat perspective taken by cyber defenders. It illustrates three elements of a threat model which are key to defining and evaluating cyber resiliency metrics. A threat model identifies the types of threats against the system or mission to be considered (e.g., adversaries, human errors, structural failures, and natural disasters). For each type of threat, characteristics and representative threat events are identified; threat events can be further characterized in terms of their consequences. For adversarial threats, characteristics include capabilities, intent, and targeting; goals (which may be directly or only indirectly related to mission) are a key aspect of intent. Adversarial threat events can also be described as adversary behaviors; multiple representative categorizations have been defined. Similarly, multiple representative characterizations of consequences have been defined. The threat model represents assumptions about the forms of adversity against which cyber resiliency is needed. These assumptions are reflected, implicitly or explicitly, in the relative priorities of cyber resiliency goals and objectives.

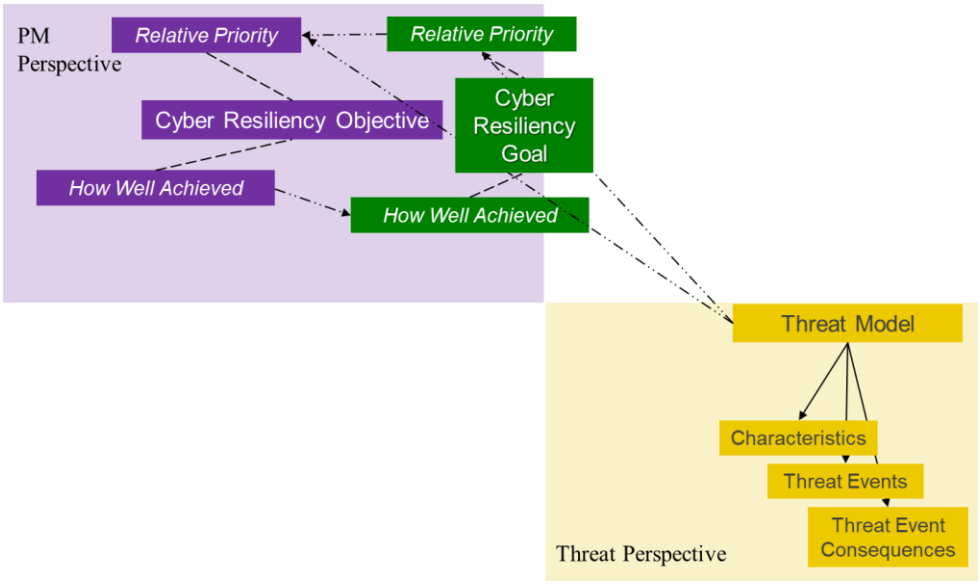

Figure 22. Cyber Resiliency Priorities Informed by Risk Factors from the Relevant Threat Model

As the next two sections describe, the mission assurance perspective and the threat perspective inform the definition of measures of effectiveness for cyber resiliency solutions, as well as the definition of more general cyber resiliency metrics or performance measures.

A.4 Measures of Effectiveness for Cyber Resiliency Solutions

As described above, a cyber resiliency solution is defined in the context of an assumed operational environment, which can range from the general (e.g., enterprise IT) to the highly specific (e.g., a specific vehicle model). That is, a cyber resiliency solution is grounded in an operational, programmatic, and threat context. A cyber resiliency solution is expected to produce *effects* – observable *changes* in system behavior or state, under assumed or specified conditions. Those conditions can include attacks as well as the occurrence of non-adversarial threat events such as user error, power failure, and fire. A measure of effectiveness is *evaluated* – that is, changes in behavior or state are observed – under actual conditions or in a representative environment, such as a modeling and simulation (M&S) environment, a laboratory, or a cyber range.

Depending on how specific the assumed operational context is and on how fully realized the evaluation environment is, a cyber resiliency solution MOE – a measure of the change resulting from applying the solution – can take many different forms. Examples include changes in

- A performance metric for an activity supporting a cyber resiliency sub-objective (and hence supporting an objective), as discussed in Section 4.1.
- A measurement made by an existing tool such as a network performance monitor or an intrusion detection system (IDS).
- The output of a cyber analytic.[27]
- A measurement made by a custom-developed tool or evaluation instrument.
- An intermediate result (e.g., assessment of threat event likelihood or consequence severity) or final result (level of risk) of a risk assessment, e.g., in the form of output from a M&S tool such as the Cyber Security Game (CSG) [58].

[27] See the Cyber Analytics Repository at https://car.mitre.org/wiki/Main_Page.

- A SME assessment of the potential severity of a threat event, changed in a way described using the Vocabulary for Describing Effects on Adversary Activities (VODEA, [76]).
- A performance metric for a VODEA-described effect on a threat event.
- A measure of performance for a mission objective, e.g., an observation made by an individual operating a CPS (e.g., whether a vehicle accelerates when the accelerator is depressed).
- An SME assessment of a risk factor (e.g., the level of adversary capabilities).
- A SME assessment of a cyber resiliency property (e.g., how well a given cyber resiliency technique or design principle is applied).

Figure 23 illustrates (using dotted lines) how a cyber resiliency solution MOE can take the form of a change in many of the metrics related to constructs discussed above.

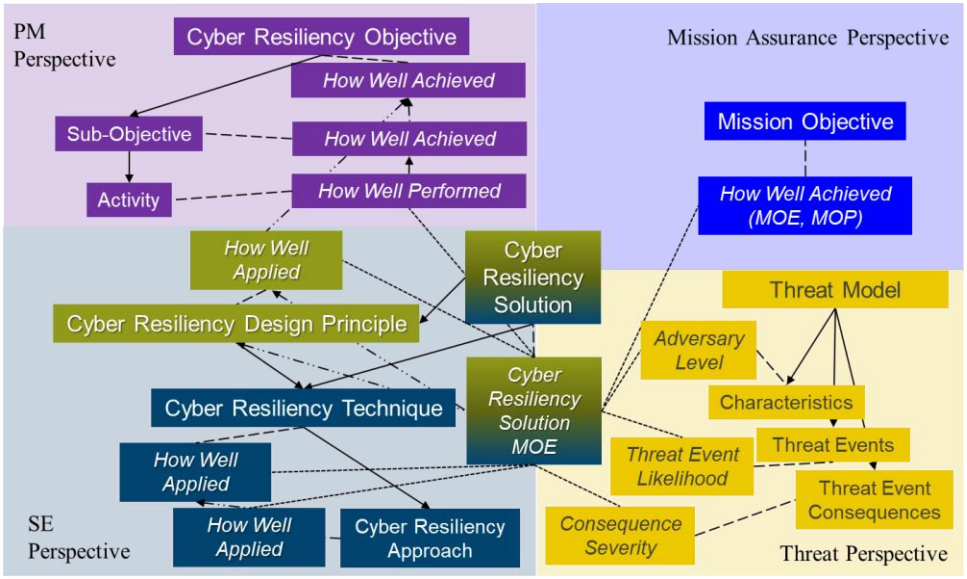

Figure 23. Relationship of Cyber Resiliency Solution MOE to Other Metrics

A.5 Characterizing Cyber Resiliency Metrics

As the discussion above indicates, definitions of cyber resiliency metrics arise in a variety of ways. A cyber resiliency metric can

- Repurpose a cyber security or cyber defense metric (e.g., number of attempted intrusions in a specified time period stopped at a network perimeter). These metrics may be quantitative, semi-quantitative, or qualitative. Cyber security or cyber defense can be viewed as a supporting mission for any cyber-dependent mission.
- Repurpose a conventional resilience metric, using the resilience reference model (e.g., length of time between initial disruption and full recovery) and mission MOEs, MOPs, or KPPs. Metrics based on the resilience reference model are typically quantitative (e.g., length of time) or semi-quantitative (e.g., level of performance, related to mission MOEs, MOPs, or KPPs). Mission MOEs and KPPs are often qualitative (e.g., yes/no), but supported by quantitative or semi-quantitative metrics (e.g., Key System Attributes or KSAs), for which threshold and target values can be established.
- Repurpose a risk metric, which may be quantitative (e.g., likelihood that a specific adversary TTP will be successful, number or percentage of compromised components) or semi-quantitative or qualitative (e.g., level of adversary capability required for successful attack, level of consequence severity).

- Express a SME judgment about a cyber resiliency property – how well a cyber resiliency objective or sub-objective is achieved, how well an activity supporting a sub-objective is performed, or how well a cyber resiliency design principle, technique, or approach is applied. These metrics are typically qualitative or semi-quantitative.
- Support a SME judgement as described above. Metrics which support SME judgments can take the form of qualitative measurements or observations (e.g., yes/no), as well as quantitative metrics which serve as indicators of or evidence for specific values produced by SME assessments. For example, the length of time since the contingency plan for an organization or mission function has been tested is an indicator of how well the Prepare objective is achieved; the absence of a documented contingency plan is evidence that the same objective is poorly or not achieved.
- Be evidence for a cyber resiliency solution, and thus identified with a cyber resiliency solution MOE. That is, an observation is made, or an attribute or behavior is measured, in order to confirm or disconfirm the expected or intended effects of a cyber resiliency solution.

A cyber resiliency solution MOE is a change in one or more of the above types of cyber resiliency metrics. The three repurposing sources of cyber resiliency metrics are informed primarily by the mission assurance and threat perspectives. SME assessments of cyber resiliency properties are informed primarily by the program manager and systems engineering perspectives. The last two sources – support for SME judgments and evidence for a cyber resiliency solution – are grounded in an assumed use case. As illustrated in Figure 24, any of the items in heavily-outlined boxes can be considered to be a cyber resiliency metrics.

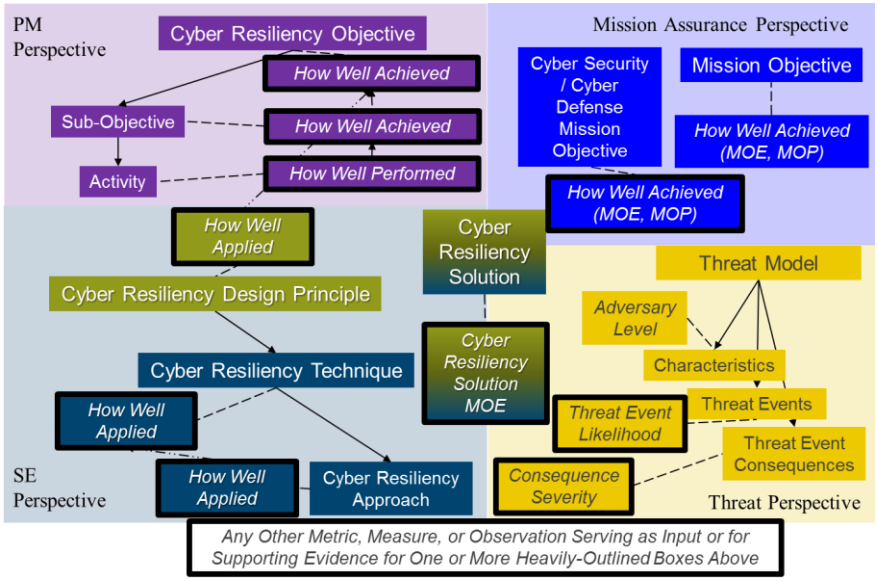

Figure 24. Many Different Metrics, Measures, or Observations Can Serve as Cyber Resiliency Metrics

Appendix B Cyber Resiliency Objective-Driven Metrics

This Appendix illustrates how cyber resiliency metrics can be defined in such a way as to be traceable to cyber resiliency objectives, as illustrated in Figure 11. As discussed in Section 3.1, metrics can be defined by identifying sub-objectives and activities (or capabilities). For each activity, one or more metrics can describe how completely, how quickly, or with what degree of confidence the activity can be performed. Those metrics can be, or can build upon, metrics defined from cyber resiliency techniques and approaches; security metrics; or conventional resilience metrics.[28] The metrics identified in this Appendix are representative; objectives must be interpreted, and sub-objectives and activities either interpreted or redefined, in the context of an overall system concept.

In the following sub-sections, sub-objectives and activities representative of a general-purpose enterprise information infrastructure are identified, with representative corresponding metrics. The cyber resiliency techniques and approaches which support each activity are also identified; note that for a given metric for an activity, only a subset of these approaches may be relevant. (For example, one activity supporting the *Restore functionality* sub-objective of the Reconstitute objective is *Coordinate recovery activities to avoid gaps in security coverage*. Some metrics are related to avoiding gaps in auditing or monitoring, while others relate to using privilege restriction to avoid gaps in access control.) As noted below, many sub-objectives and activities are also relevant to cyber-physical systems, and some are relevant to CPS or PIT as deployed in a detached or restricted-connectivity environment.

To facilitate tracking, the activities have been assigned identifiers of the form OO-S#-A#, where OO indicates the objective (PA for Prevent / Avoid, PR for Prepare, CN for Continue, CS for Constrain, RE for Reconstitute, UN for Understand, TR for Transform, and RA for Re-Architect), S# indicates the sub-objective, and A# indicates the activity. A final number is assigned to identify the metric (e.g., RE-S1-A3-1 is the first metric defined for the third activity supporting the first sub-objective for the Reconstitute objective). Metric identifiers reflect the corresponding entries in the Cyber Resiliency Metrics Catalog [11].

B.1 Prevent / Avoid

The Prevent / Avoid objective – *Preclude the successful execution of an attack or the realization of adverse conditions* – has four representative sub-objectives:

1. Apply basic hygiene and risk-tailored controls. This sub-objective is consistent with the philosophy of the Risk Management Framework (RMF), in which controls are selected and applied to resources based on identified risk factors, particularly on sensitivity, criticality, and trustworthiness.
2. Limit exposure to threat events.
3. Decrease the adversary's perceived benefits.
4. Modify configurations based on threat intelligence.

The first three sub-objectives do not require active human intervention, and thus apply to all types of systems; however, many representative activities do involve the efforts of system administrators or cyber

[28] The metrics identified in this Appendix are included in the Cyber Resiliency Metrics Catalog. As discussed in [11], some metrics in the catalog are carried over from an earlier version [10] and have identifiers of the form MT-#. Others are metrics related to techniques and implementation approaches; for example, metrics with the identifier RD-RE-# are related to the Replication implementation approach to the Redundancy technique.

defenders. The last sub-objective does strongly involve cyber defender efforts, and thus is not representative of unfederated CPS or of PIT operating in stand-off mode[29].

Representative activities and metrics related to these sub-objectives are identified below.

Table 6. Prevent / Avoid: Apply basic hygiene and risk-tailored controls

Sub-Objective: Apply basic hygiene and risk-tailored controls	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
PA-S1-A1: Restrict access to resources based on criticality and sensitivity (i.e., on resource attractiveness to adversaries)[30] *[Privilege Restriction: Trust-Based Privilege Management, Attribute-Based Usage Restriction; Segmentation: Predefined Segmentation]*	Percentage of cyber resources to which access is controlled based on criticality [PA-S1-A1-2] Percentage of cyber resources to which access is controlled based on sensitivity [PA-S1-A1-3] Percentage of users with privileged/administrator access [PA-S1-A1-4] Percentage of [administrative, operational] activities [procedurally, technically] enforced by 2-person controls [PA-S1-A1-5]
PA-S1-A2: Restrict behaviors of users and cyber entities (e.g., components, services, processes, interfaces) based on degree of trust *[Privilege Restriction: Trust-Based Privilege Management, Attribute-Based Usage Restriction]*	Percentage of users for which behaviors are restricted based on assigned degree of trust [PA-S1-A2-1] Percentage of types of cyber entities for which behaviors are restricted based on assigned degree of trust [PA-S1-A2-2]
PA-S1-A3: Enforce clear boundaries on sets of cyber resources *[Segmentation: Predefined Segmentation, Realignment: Purposing]*	Percentage of cyber resources which can be placed in a single enclave [PA-S1-A3-1] Percentage of cyber resources which have been placed in a single enclave [PA-S1-A3-2] Percentage of cyber resources which can be discovered, accessed or used, or otherwise reached from another enclave [PA-S1-A3-3] Number of dedicated operational enclaves (i.e., enclaves dedicated to a mission or business function) defined [PA-S1-A3-4] Number of dedicated administrative enclaves defined [PA-S1-A3-5] Number of dedicated security/audit enclaves define [PA-S1-A3-6] Percentage of enclaves associated with a single operational function [PA-S1-A3-7]
PA-S1-A4: Apply multiple defenses to critical assets *[Coordinated Protection: Calibrated Defense-in-Depth, Orchestration]*	Percentage of critical cyber resources to which multiple defenses are applied [PA-S1-A4-1]
PA-S1-A5: Protect data in different states (e.g., at rest, in transit, in processing) *[Deception: Obfuscation]*	Percentage of external communications which are encrypted [PA-S1-A5-1] Percentage of internal communications which are encrypted [PA-S1-A5-2] Percentage of information stores which are encrypted [PA-S1-A5-3] Percentage of processing which is encrypted or obfuscated [PA-S1-A5-4] *Note: Percentages may be more granular, based on different levels of information sensitivity.* Strength of encryption mechanism for [external communications | internal communications | information stores | processing] [PA-S1-A5-5]

[29] A system accessed using a networking method only intermittently (e.g., via a low-power connection to check the status of an insulin pump; via a wired connection to upgrade software in an embedded avionic device) is said to operate in stand-off mode when not connected to a network.

[30] Note that this activity depends on UN-S2-A1, Perform impact analysis to identify critical assets / capabilities.

Sub-Objective: Apply basic hygiene and risk-tailored controls	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
PA-S1-A6: General (assumes standard practices for vulnerability scanning and patching)	Average length of time to patch systems [MT-38] Average length of time to patch network components [MT-41] Percentage of systems in compliance with organizationally mandated configuration guidance [MT-39] Percentage of managed systems checked for vulnerabilities in accordance with the organization's policy [MT-55] Percentage of systems without "high" severity vulnerabilities based on Common Vulnerability Scoring System (CVSS) scoring [MT-56] Average length of time for the organization to mitigate identified vulnerabilities [MT-57] Percentage of managed systems for which an automated patch management process is used [MT-58] Average length of time from patch release to patch installation [MT-60] Percentage of cyber resources that are properly configured [MT-1] Frequency of audit record analysis for inappropriate activity [MT-42] Percentage of systems for which a defined security configuration is required [MT-62]
PA-S1-A7: General (assumes good practices for training, documentation, and environmental controls)	Percentage of personnel who successfully completed annual security training [MT-63] Degree to which system operators deviate from documented cyber resiliency guidance and procedures [MT-98] Level of access limitation for external maintenance personnel [MT-121]

Table 7. Prevent / Avoid: Limit exposure to threat events

Sub-Objective: Limit exposure to threat events	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
PA-S2-A1: Identify and implement a set of change parameters (e.g., conditions under which changes should not be made, range within which a service may be moved, ranges for frequency of changes) *[Coordinated Protection: Consistency Analysis]*	Percentage of configuration parameters for which allowable ranges have been defined [PA-S2-A1-1] Percentage of CCoAs which make changes within allowable ranges [PA-S2-A1-2] Percentage of automated change mechanisms for which changes can be restricted to allowable ranges [PA-S2-A1-3] Percentage of change parameters permitted to control unpredictability, outside of a schedule [PA-S2-A1-4]
PA-S2-A2: Switch to an alternative resource randomly or in response to a triggering event *[Adaptive Response: Dynamic Reallocation; Redundancy: Replication; Unpredictability: Contextual Unpredictability, Temporal Unpredictability]*	Percentage of resources for which an alternative exists [RD-RE-1] Percentage of critical resources for which multiple (more than one) alternatives exist [RD-RE-2] Percentage of resources for which an alternative exists for which switching is performed [PA-S2-A2-1] Percentage of resources switches enabled by random vs. triggered events [PA-S2-A2-2] Average time to complete the switching process (latency or lag) [PA-S2-A2-3] Average frequency of switches to an alternative resource per unit time [PA-S2-A2-4]

Sub-Objective: Limit exposure to threat events	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
PA-S2-A3: Create and switch to an alternative version of process or service randomly or in response to a triggering event *[Adaptive Response: Adaptive Management; Diversity: Synthetic Diversity; Unpredictability: Contextual Unpredictability, Temporal Unpredictability]*	Percentage of processes or services for which an alternative version can be instantiated [RD-RE-3] Percentage of processes or services for which an alternative version can be instantiated for which instantiation is performed [PA-S2-A3-1] Average time to complete the process of instantiating and switching to an alternative version of a process or service [PA-S2-A3-2] Average frequency of switches to an alternative version of a process or service per unit time [PA-S2-A3-3]
PA-S2-A4: Reconfigure components and services randomly or in response to a triggering event *[Adaptive Response: Dynamic Reconfiguration; Unpredictability: Contextual Unpredictability, Temporal Unpredictability]*	Percentage of resources for which configuration changes can be made dynamically [PA-S2-A4-1] Percentage of resources to which configuration changes can be made randomly or in response to a triggering event [PA-S2-A4-2] Percentage of such resources for which changes are made randomly or in response to a triggering event [PA-S2-A4-3] Average time to complete the dynamic reconfiguration process (latency or lag) [PA-S2-A4-4] Frequency of configuration changes per unit time [PA-S2-A4-5]
PA-S2-A5: Dynamically relocate processing randomly or in response to a triggering event *[Adaptive Response: Dynamic Reconfiguration; Dynamic Positioning: Asset Mobility, Functional Relocation of Cyber Resources; Unpredictability: Contextual Unpredictability, Temporal Unpredictability]*	Percentage of services which can be relocated virtually (e.g., to another virtual machine) [DP-FR-1] Percentage of resources which can be virtually relocated automatically [DP-FR-2] Percentage of resources which can be relocated physically (e.g., to a backup facility) [DP-AM-1] Percentage of resources which can be physically relocated automatically [DP-AM-2] Percentage of resources which can be relocated virtually which are relocated [PA-S2-A5-1] Percentage of resources which can be relocated physically which are relocated [PA-S2-A5-2] Average time to complete the virtual relocation process (latency or lag) [DP-FR-3] Average time to complete the physical relocation process (latency or lag) [DP-AM-3] Frequency of relocation events per unit time [PA-S2-A5-3]
PA-S2-A6: Retain resources in an active or "live" state for a limited lifespan (e.g., maximum time period after instantiation or creation, maximum period after use) *[Non-Persistence: Non-Persistent Services, Non-Persistent Connectivity, Non-Persistent Information]*	Percentage of communications paths to which lifespan conditions are applied [PA-S2-A6-1] Percentage of mission services to which lifespan conditions are applied [PA-S2-A6-2] Percentage of supporting services to which lifespan conditions are applied [PA-S2-A6-3] Percentage of information resources to which lifespan conditions are applied [PA-S2-A6-4] Percentage of lifespan conditions determined based on threat intelligence or known adversarial TTPs [PA-S2-A6-5] Maximum or average lifespan of a communications path [PA-S2-A6-6] Maximum or average lifespan of a mission service [PA-S2-A6-7] Maximum or average lifespan of a supporting service [PA-S2-A6-8] Maximum or average lifespan of an information resource [PA-S2-A6-9]

Sub-Objective: Limit exposure to threat events	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
PA-S2-A7: Ensure that termination, deletion, or movement does not leave residual mission critical or sensitive data or software behind *[Dynamic Positioning: Functional Relocation of Cyber Resources; Non-Persistence: Non-Persistent Services, Non-Persistent Information]*	Amount of [mission critical, sensitive] information which can be retrieved or reconstructed by a Red Team after a service is moved or terminated (as percentage of amount of information which can be obtained by a Red Team if the service is not moved or terminated) [PA-S2-A7-1] Amount of information which can be retrieved or reconstructed by a Red Team after an information resource is deleted (as a percentage of amount of information in the resource prior to deletion) [PA-S2-A7-2]
PS-SA-A8: Separate cyber resources based on criticality and/or sensitivity *[Segmentation: Predefined Segmentation]*	Percentage of mission-critical cyber resources which can be discovered or reached from each enclave, sub-system, or network nodes [PA-S2-A8-1] Percentage of high-sensitivity information stores which can be discovered or reached from all sub-systems or network nodes [PA-S2-A8-2]
PA-S2-A9: Split or distribute cyber resources across multiple locations to avoid creating high-value targets *[Dynamic Positioning: Fragmentation, Distributed Functionality]*	Percentage of high-sensitivity or high-criticality information stores which are fragmented across multiple locations [PA-S2-A9-1] Number of geographically diverse locations included in the fragmentation set [PA-S2-A9-2] Percentage of mission-critical functions which are executed by distributed rather than centralized services [PA-S2-A9-3]
PA-S2-A10: Modify privilege restrictions unpredictably *[Privilege Restriction: Dynamic Privileges; Unpredictability: Temporal Unpredictability, Contextual Unpredictability]*	Percentage of cyber resources for which privileges can be modified dynamically [PV-DP-1] Percentage of such resources for which privileges are modified randomly [PA-S2-A10-1] Percentage of users for whom privileges can be modified dynamically [PV-DP-2] Percentage of such users whose privileges are modified dynamically [PA-S2-A10-2] Percentage of system services for which privileges can be modified randomly [PV-DP-3] Percentage of such resources for which privileges are modified randomly [PA-S2-A10-3]

Table 8. Prevent / Avoid: Decrease the adversary's perceived benefits

Sub-Objective: Decrease the adversary's perceived benefits	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
PA-S3-A1: Conceal resources an adversary might find attractive *[Deception: Obfuscation]*	Percentage of sensitive data stores that are encrypted [PA-S3-A1-1] Strength of encryption used to protect sensitive data stores [PA-S3-A1-2] Percentage of data streams used for sensitive data that are encrypted [PA-S3-A1-3] Strength of encryption used to protect sensitive data streams [PA-S3-A1-4] Time for a Red Team to identify which critical resources are involved in mission processing [PA-S3-A1-5]
PA-S3-A2: Present misleading information about information, resources, and capabilities *[Deception: Dissimulation, Misdirection]*	Number of external venues in which misleading or false information is presented [PA-S3-A2-1] Number of internal venues in which misleading or false information is presented [PA-S3-A2-1] Frequency of updates to misleading or false information [PA-S3-A2-3] Time since last update of misleading or false information [PA-S3-A2-4] Number of attempted intrusions deflected to a honeypot [MT-4] Adversary dwell time in deception environment [MT-264] Percentage of attackers in a deception environment who are unaware of their containment [MT-265]

Table 9. Prevent / Avoid: Modify configurations based on threat intelligence

Sub-Objective: Modify configurations based on threat intelligence	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
PA-S4-A1: Modify allocation of resources and assignment of privileges and access / usage restrictions based on threat indications and warning (I&W) *[Adaptive Response: Dynamic Reconfiguration, Dynamic Resource Allocation, Adaptive Management; Privilege Restriction: Dynamic Privileges]*	Percentage of resources to which dynamic changes can be made [PA-S4-A1-1] Percentage of resources for which dynamic changes are made in response to I&W [PA-S4-A1-2] Time to propagate modifications to all resources which should be affected [PA-S4-A1-3]
PA-S4-A2: Coordinate definition and assignment of privileges to eliminate opportunities for privilege escalation *[Coordinated Protection: Consistency Analysis; Privilege Restriction: Trust-Based Privilege Management, Dynamic Privileges]*	Time since last scrub of privilege definition and assignment [PA-S4-A2-1] Frequency of review of privileged definition and assignment [PA-S4-A2-2] Random reviews performed on privilege definitions/assignments [yes/no] [PA-S4-A2-3] Number of distinct privileges which can be assigned to an individual or process [PA-S4-A2-4] Complexity of the set of privileges, when represented as a partially directed graph [PA-S4-A2-5] Percentage of users assigned to each privilege [PA-S4-A2-6] Percentage of users with access to [read, modify] critical resources or sensitive information [PA-S4-A2-7] Percentage of administrators who can administer both network and security components [MT-123]

Sub-Objective: Modify configurations based on threat intelligence	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
PA-S4-A3: General	Percentage of information system security personnel that have received security training [MT-40] Percentage of DNS servers under the organization's control that have been hardened [MT-134] Percentage of enterprise DNS servers to which Domain Name System Security (DNSSEC) extensions have been applied [MT-135]

B.2 Prepare

The Prepare objective – *Maintain a set of realistic courses of action that address predicted or anticipated adversity* – has three representative sub-objectives:

1. Create and maintain cyber courses of action.
2. Maintain the resources needed to execute cyber courses of action. Resources include not only cyber resources, but also personnel (with the proper training) and procedures.
3. Validate the realism of cyber courses of action. Validation methods include testing or exercises.

Because CCoAs can be automated, these sub-objectives apply to all types of systems, even unfederated CPS or PIT operating in stand-off mode. However, activities which involve a cyber playbook or efforts by an organization or by cyber defenders do not.

Representative activities and metrics related to these sub-objectives are identified below.

Table 10. Prepare: Create and maintain cyber courses of action

Sub-Objective: Create and maintain cyber courses of action	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
PR-S1-A1: Define and implement automated CCoAs *[Adaptive Response: Adaptive Management; Coordinated Protection: Orchestration]*	Percentage of cyber resources which can be defended by automated CCoAs [PR-S1-A1-1] Percentage of identified threat types, categories of threat actions, or TTPs [with reference to an identified threat model] for which automated CCoAs are defined [PR-S1-A1-2] Percentage of individually managed systems having a defined mode for degraded operation [MT-85]
PR-S1-A2: Define / maintain a cyber playbook containing realistic CCoAs, i.e., CCoAs that can be executed in a coordinated way given existing controls and management responsibilities *[Coordinated Protection: Consistency Analysis, Orchestration]*	Number of CCoAs documented in the organization's cyber playbook [PR-S1-A2-1] Percentage of identified threat types, categories of threat actions, or TTPs [with reference to an identified threat model] addressed by at least one CCoA in the cyber playbook [PR-S1-A2-2] Percentage of potential classes of cyber effects addressed by at least one CCoA in the cyber playbook [PR-S1-A2-3] Time since last update of the organization's cyber playbook [PR-S1-A2-4] Frequency of CCoA review/updates [PR-S1-A2-5] Percentage of mission-essential functions for which a procedural work-around is available [MT-7] Percentage of information systems for which annual testing of contingency plans has been conducted [MT-44] Degree of consistency between organizational threat-response policies for system managers and organizational threat-response policies for operators [MT-95]

Sub-Objective: Create and maintain cyber courses of action	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
PR-S1-A3: Track effectiveness of CCoAs and adapt as necessary *[Adaptive Response: Adaptive Management; Coordinated Protection: Consistency Analysis, Orchestration]*	Percentage of CCoAs for which MOEs are defined [PR-S1-A3-1] Percentage of CCoAs for which MOEs are tracked [PR-S1-A3-2] Average time between the exercise of a CCoA and its update [PR-S1-A3-3] For each possible effect on threat event, the number of CCoAs which are expected to have that effect [PR-S1-A3-4] Additional / diverted level of effort to maintain mission-essential functions for a given CCoA [MT-10]

Table 11. Prepare: Maintain the resources needed to execute cyber courses of action

Sub-Objective: Maintain the resources needed to execute cyber courses of action	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
PR-S2-A1: Back up data needed to restore or reconstitute mission and supporting functionality *[Redundancy: Protected Backup and Restore]*	Percentage of cyber resources which are backed up [PR-S2-A1-1] Percentage which are backed up into hot backups [PR-S2-A1-2] Percentage which are backed up into cold / archival storage [PR-S2-A1-3] Time since restoration / reconstitution processes were last exercised [PR-S2-A1-4] Average time to restore [PR-S2-A1-5] Average time to back up [PR-S2-A1-6] Frequency of backup [PR-S2-A1-7] Frequency at which key information assets are replicated to a backup data store or standby system through database journaling [MT-183]
PR-S2-A2: Pre-position resources to support CCoAs *[Coordinated Protection: Calibrated Defense-in-Depth, Orchestration; Redundancy: Surplus Capacity, Replication]*	Percentage of those CCoAs for which alternative resources (e.g., at a standby site) identified in the CCoA are available [PR-S2-A2-1] Elapsed time since a spot check of the availability of alternate resources for each CCoA has been performed [PR-S2-A2-2] Percentage of those CCoAs for which staff identified in the CCoA have been trained in their responsibilities with respect to the CCoA [PR-S2-A2-3] Average time since last staff training with respect to the CCoA [PR-S2-A2-4]
PR-S2-A3: Maintain gold copies of mission-essential software and configuration data *[Redundancy: Protected Backup and Restore]*	Percentage of mission-essential software (with supporting configuration data) for which a gold copy exists [PR-S2-A3-1] Time since last update of the gold copy [PR-S2-A3-2] Time since last validation of the gold copy [PR-S2-A3-3] Time taken between system updates and generation of gold copy [PR-S2-A3-4]
PR-S2-A4: Provide mechanisms and/or procedures for snapshotting or otherwise capturing, and then restoring, state *[Analytic Monitoring: Malware and Forensic Analysis]*	Percentage of information or processing resources which can be snapshot, expunged, and restored to a known good state [PR-S2-A4-1] Time since snapshotting and restoration mechanisms have been last exercised [PR-S2-A4-2] Can snapshot be performed live [yes/no] [PR-S2-A4-3]
PR-S2-A5: Maintain multiple protected instances of hardware *[Diversity: Supply Chain Diversity; Redundancy: Replication]*	Percentage of mission-critical hardware components for which protected alternates are maintained [PR-S2-A5-1] Number of protected alternates for a given mission-critical hardware component [PR-S2-A5-2] Degree of confidence in protection of alternate component (based on supply chain risk management (SCRM) controls) [PR-S2-A5-3] Percentage of hot vs cold/spare components for mission-critical hardware [PR-S2-A5-4]

Sub-Objective: Maintain the resources needed to execute cyber courses of action	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
PR-S2-A6: Acquire and maintain architectural alternatives for key system elements (e.g., OSs, browsers) *[Diversity: Architectural Diversity]*	Percentage of key system elements for which architectural alternatives are maintained [PR-S2-A6-1] Number of architectural alternatives for each type of key system element [PR-S2-A6-2]
PR-S2-A7: Define and maintain determinably different alternative processing paths (i.e., different sequences of services or applications used to respond to the same request) *[Diversity: Design Diversity]*	Percentage of mission-essential capabilities for which two or more different instantiations are available [MT-8] Number of alternate instantiations of a required capability that can be deployed [MT-33] Percentage of mission / business process threads for which alternative processing paths are available [PR-S2-A7-1] Time since last exercise of alternative processing paths for a given mission / business process thread [PR-S2-A7-2] Frequency of alternate path usage [PR-S2-A7-3]
PR-S2-A8: Define and maintain determinably different alternative communications paths (e.g., different protocols, different communications media) *[Diversity: Path Diversity]*	Percentage of communications paths for which alternatives are available [PR-S2-A8-1] Time since last exercise of alternative communications paths [PR-S2-A8-2]
PR-S2-A9: Use determinably different supply chains for key technical components *[Diversity: Supply Chain Diversity]*	Percentage of mission-critical technical components for which diverse supply chains are used [PR-S2-A9-1] Frequency of SCRM review [PR-S2-A9-2] Percentage of components with verified supply chain integrity [PR-S2-A9-3]
PR-S2-A10: Identify and maintain determinably different mission data sources *[Diversity: Information Diversity]*	Percentage of mission-critical data stores for which diverse data sources are available [PR-S2-A10-1] Percentage of mission-essential datasets for which all items effectively have two or more independent external data feeds [MT-14] Percentage of data value assertions in a mission-essential data store for which two or more different data feeds are available [MT-15]
PR-S2-A11: Create and maintain determinably different information stores *[Diversity: Information Diversity]*	Percentage of mission-critical data types for which multiple different data stores are maintained [PR-S2-A11-1] Percentage of diverse datastores using unique technologies (e.g., SQL vs. noSQL) [PR-S2-A11-2]
PR-S2-A12: Create and maintain multiple protected instances of information *[Diversity: Information Diversity; Redundancy: Replication]*	Percentage of mission-critical data stores for which a gold copy is maintained [MT-16] Percentage of data value assertions in a mission-essential data store for which a master copy exists [MT-17] Percentage of mission-critical data stores for which at least two gold copies (one current, one as-of a given prior date) are maintained [PR-S2-A12-1] Number and age of maintained gold copies[PR-S2-A12-2]
PR-S2-A13: Create and maintain multiple protected instances of software *[Diversity: Design Diversity, Synthetic Diversity; Redundancy: Replication]*	Percentage of mission-critical software components for which a gold copy is maintained [PR-S2-A13-1] Percentage of mission-critical software components for which at least two gold copies (current, and previous) are maintained [PR-S2-A13-2] Number and age of maintained gold copies [PR-S2-A13-3] Percentage of virtual machine (VM) images available for download for which alternative codebases exist [MT-202]

Table 12. Prepare: Validate the realism of cyber courses of action

Sub-Objective: Validate the realism of cyber courses of action	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
PR-S3-A1: Validate expected dependencies and interactions among cyber defenses, security controls, and performance controls *[Coordinated Protection: Consistency Analysis, Orchestration, Self-Challenge; Contextual Awareness: Dynamic Resource Awareness, Mission Dependency and Status Visualization]*	Percentage of security controls or security administrative functions mapped to CCoAs which rely on those controls or functions [PR-S3-A1-1] Percentage of performance controls or performance management functions mapped to CCoAs which rely on those controls or functions [PR-S3-A1-2]
PR-S3-A2: Simulate and/or exercise CCoAs *[Coordinated Protection: Self-Challenge]*	Time since last [random, scheduled] exercise or simulation of one or more CCoAs [PR-S3-A2-1] Time since last [random, scheduled] exercise or simulation of all CCoAs in the organization's cyber playbook [PR-S3-A2-2] Frequency of exercise [PR-S3-A2-3] Exercises performed on live system [yes/no] [PR-S3-A2-4] Exercises performed randomly [yes/no] [PR-S3-A2-5] Time since last exercise [PR-S3-A2-6] Frequency of joint exercises [PR-S3-A2-7]

B.3 Continue

The Continue objective – *Maximize the duration and viability of essential mission or business functions during adversity* – has three representative sub-objectives:

1. Minimize degradation of service delivery.
2. Minimize interruptions in service delivery.
3. Ensure that ongoing functioning is correct.

These sub-objectives apply to all types of systems. However, for each sub-objective, some activities involve efforts by an organization or by cyber defenders; those activities are not representative of unfederated CPS or of PIT operating in stand-off mode.

Some activities are common to multiple sub-objectives of both the Continue and Constrain objectives. These relate to damage assessment, selecting and tailoring cyber courses of action, and validating integrity or correct behavior.

Representative activities and metrics related to these sub-objectives are identified below.

Table 13. Continue: Minimize degradation of service delivery

Sub-Objective: Minimize degradation of service delivery	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
CN-S1-A1: Perform mission damage assessment[31] *[Analytic Monitoring: Monitoring and Damage Assessment; Contextual Awareness: Mission Dependency and Status Visualization; Substantiated Integrity: Integrity Checks, Behavior Validation]*	Elapsed time for mission damage assessment [AM-DA-1] Average, median, or maximum time required to validate the integrity and/or quality of mission-critical data [SI-IC-1] Percentage of mission-critical data assets for which data integrity / quality can be validated [SI-IC-2] Percentage of mission-critical data assets for which data integrity / quality has been validated since initiation of CCoA [CN-S1-A1-1] Average, median, or maximum time required to validate the integrity and/or quality of security-critical data [SI-IC-3] Average, median, or maximum time required to validate the integrity and/or behavior of mission-critical services or processes [SI-BV-1] Percentage of mission-critical applications for which integrity / behavior has been validated since initiation of CCoA [CN-S1-A1-2] Average, median, or maximum time required to validate the integrity and/or behavior of security-critical services or processes [SI-BV-2] Percentage of security-critical applications for which integrity / behavior has been validated since initiation of CCoA [CN-S1-A1-3] Frequency of software/service integrity check [SI-IC-5]
CN-S1-A2: Maintain acceptable levels of performance for mission-critical, security-critical, and mission-supporting applications and services *[Adaptive Response: Adaptive Management; Contextual Awareness: Mission Dependency and Status Visualization]*	Degree of degradation of a specific mission-essential function (or set of functions) [MT-12] Length of time between initial disruption and availability (at minimum level of acceptability) of mission-essential functions [MT-13] Percentage of mission-critical applications and services for which MOPs remain at or above their required levels [for the duration of the mission task they support | for the duration of the mission they support | for the (specified) time period] [CN-S1-A2-1] Percentage of pre-disruption availability / performance after disruption [MT-21] Percentage of security-critical applications and services for which MOPs remain at or above their required levels over (specified) time period [CN-S1-A2-2] Percentage of mission-supporting applications and services for which MOPs remain at or above their required levels [for the duration of the mission task they support | for the duration of the mission they support | for the (specified) time period] [CN-S1-A2-3]
CN-S1-A3: Select and tailor CCoA *[Adaptive Response: Adaptive Management; Contextual Awareness: Mission Dependency and Status Visualization]*	Time between selection of CCoA and completion of tailoring [CN-S1-A3-1] Time between determination that a CCoA must be taken and initiation of tailored CCoA [CN-S1-A3-2]
CN-S1-A4: Dynamically reconfigure existing resources *[Adaptive Response: Dynamic Reconfiguration]*	Percentage of cyber resources which can be reconfigured on demand [CN-S1-A4-1] Time between decision to reconfigure resources and completion of reconfiguration [CN-S1-A4-2] Percentage of cyber resources which can be [automatically, manually] reconfigured [CN-S1-A4-3]

[31] Mission damage is the decrease in the ability to complete the current mission and to accomplish future missions, and may be assessed in terms of mission measures of effectiveness (MOEs), system measures of performance (MOPs), or Key Performance Parameters (KPPs) of system elements.

Sub-Objective: Minimize degradation of service delivery	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
CN-S1-A5: Dynamically provision by reallocating existing resources *[Adaptive Response: Dynamic Reallocation; Redundancy: Surplus Capacity]*	Percentage of cyber resources which can be reallocated on demand [CN-S1-A5-1] Time between decision to reallocate resources and completion of reallocation [CN-S1-A5-2]
CN-S1-A6: Dynamically recreate critical capabilities by combining existing resources in a novel way *[Adaptive Response: Dynamic Reconfiguration]*	Percentage of critical capabilities which can be recreated by combining existing resources in a novel way [CN-S1-A6-1] Time between decision to recreate resources and completion of the process [CN-S1-A6-2]
CN-S1-A7: Relocate resources to minimize service degradation *[Adaptive Response: Adaptive Management; Dynamic Positioning: Asset Mobility, Functional Relocation of Cyber Resources]*	Time between decision to relocate resources and completion of relocation [CN-S1-A7-1] Percentages of services which can be relocated virtually (e.g., to another virtual machine) [DP-FR-1] Percentage of services which can be automatically relocated virtually [DP-FR-2] Percentage of resources which can be relocated physically (e.g., to a backup facility) [DP-AM-1] Percentage of resources which can be relocated automatically [DP-AM-2] Frequency with which relocation occurs [CN-S1-A7-2]
CN-S1-A8: General	Percentage of pre-disruption availability / performance after disruption [MT-21]

Table 14. Continue: Minimize interruptions in service delivery

Sub-Objective: Minimize interruptions in service delivery	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
CN-S2-A1: Perform mission damage assessment *[Analytic Monitoring: Monitoring and Damage Assessment; Contextual Awareness: Mission Dependency and Status Visualization; Substantiated Integrity: Integrity Checks, Behavior Validation]*	Elapsed time for mission damage assessment [AM-DA-1] Average, median, or maximum time required to validate the integrity and/or quality of mission-critical data [SI-IC-1] Percentage of mission-critical data assets for which data integrity / quality can be validated [SI-IC-2] Percentage of mission-critical data assets for which data integrity / quality has been validated since initiation of CCoA [CN-S1-A1-1] Average, median, or maximum time required to validate the integrity and/or quality of security-critical data [SI-IC-3] Average, median, or maximum time required to validate the integrity and/or behavior of mission-critical services or processes [SI-BV-1] Percentage of mission-critical applications for which integrity / behavior has been validated since initiation of CCoA [CN-S1-A1-2] Average, median, or maximum time required to validate the integrity and/or behavior of security-critical services or processes [SI-BV-2] Percentage of security-critical applications for which integrity / behavior has been validated since initiation of CCoA [CN-S1-A1-3] Frequency of software/service integrity check [SI-IC-5]
CN-S2-A2: Select and tailor CCoA *[Adaptive Response: Adaptive Management; Contextual Awareness: Mission Dependency and Status Visualization]*	Time between selection of CCoA and completion of tailoring [CN-S2-A2-1] Time between determination that a CCoA must be taken and initiation of tailored CCoA [CN-S2-A2-2]

Sub-Objective: Minimize interruptions in service delivery	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
CN-S2-A3: Coordinate response activities to ensure synergy rather than interference *[Coordinated Protection: Orchestration]*	Percentage of responsible organizational entities which have established points of contact, primary and alternative lines of communication, and documented procedures for responding to a cyber incident [CN-S2-A3-1] Time since last exercise [PR-S3-A2-6] Frequency of joint exercises [PR-S3-A2-7]
CN-S2-A4: Deploy diverse resources rapidly (e.g., in near real time) *[Adaptive Response: Dynamic Reconfiguration, Diversity: Architectural Diversity, Design Diversity, Synthetic Diversity, Path Diversity]*	Time between decision to redeploy resources and completion of redeployment [CN-S2-A4-1] Number of differences between initial set of resources and redeployed set [CN-S2-A4-2]
CN-S2-A5: Fail over to replicated resources *[Adaptive Response: Dynamic Reconfiguration; Redundancy: Protected Backup and Restore, Replication]*	Average, median, or maximum time to fail over mission-critical functions over [specify period over which measurements are taken] [CN-S2-A5-1] Percentage of failovers which met required MOPs during [specify period over which measurements are taken] [CN-S2-A5-2] Time since last test of failover [CN-S2-A5-3] Length of time to deploy redundant resources [MT-29] Length of time to bring a backup server online [MT-159]
CN-S2-A6: Replace suspect hardware components with protected alternates *[Adaptive Response: Dynamic Reconfiguration; Diversity: Supply Chain Diversity; Redundancy: Replication]*	Time to replace a mission-critical hardware component with a protected alternate [CN-S2-A6-1] Confidence that alternate is not affected by similar issues [CN-S2-A6-2]
CN-S2-A7: Switch processing to use alternative processing paths (i.e., different sequences of services or applications used to respond to the same request) *[Adaptive Response: Dynamic Reconfiguration; Diversity: Design Diversity]*	Average, median, or maximum time to switch a mission-critical function to an alternative processing path [CN-S2-A7-1] Frequency of use/test of alternative processing paths CN-S2-A7-2]
CN-S2-A8: Switch communications to use alternative communications paths (e.g., different protocols, different communications media) *[Adaptive Response: Dynamic Reconfiguration; Diversity: Path Diversity]*	Average, median, or maximum time to switch a mission-critical connection to an alternative communications path [CN-S2-A8-1] Frequency of use/test of alternative communications paths [CN-S2-A8-2]
CN-S2-A9: Locate and switch over to alternative mission data sources *[Adaptive Response: Dynamic Reconfiguration; Diversity: Information Diversity]*	Average, median, or maximum time to locate and switch over to an alternative mission data source [CN-S2-A9-1]
CN-S2-A10: Locate and switch over to alternative information stores *[Adaptive Response: Dynamic Reconfiguration; Diversity: Information Diversity]*	Average, median, or maximum time to locate and switch over to an alternative information store [CN-S2-A10-1]

Table 15. Continue: Ensure that ongoing functioning is correct

Sub-Objective: Ensure that ongoing functioning is correct	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
CN-S3-A1: Validate provenance of mission-critical and system control data *[Substantiated Integrity: Provenance Tracking]*	Average, median, or maximum time required to validate the provenance of mission-critical and system control data [SI-PT-1] Percentage of mission-critical and system control data for which provenance can be validated [SI-PT-2] Percentage of mission-critical and system control data for which provenance has been validated since the initiation of the CCoA [CN-S3-A1-1] Average, median, or maximum time required to validate the provenance of security-critical data [SI-PT-3] Percentage of security-critical data for which provenance can be validated [SI-PT-4] Percentage of security-critical data for which provenance has been validated since the initiation of the CCoA [CN-S3-A1-2]
CN-S3-A2: Validate data integrity / quality to ensure it has not been corrupted *[Substantiated Integrity: Integrity Checks]*	Average, median, or maximum time required to validate the integrity and/or quality of mission-critical data [SI-IC-1] Percentage of mission-critical data assets for which data integrity / quality can be validated since initiation [SI-IC-2] Percentage of mission-critical data assets for which data integrity / quality has been validated since initiation of CCoA [CN-S1-A1-1] Average, median, or maximum time required to validate the integrity and/or quality of security-critical data [SI-IC-3] Number of points in a mission thread where mission-critical data is validated in support of an operation [SI-IC-4]
CN-S3-A3: Validate software / service integrity / behavior to ensure it has not been corrupted *[Substantiated Integrity: Integrity Checks, Behavior Validation]*	Average, median, or maximum time required to validate the integrity and/or behavior of mission-critical services or processes [SI-BV-1] Percentage of mission-critical applications for which integrity / behavior has been validated since initiation of CCoA [CN-S1-A2-2] Average, median, or maximum time required to validate the integrity and/or behavior of security-critical services or processes [SI-BV-2] Percentage of security-critical applications for which integrity / behavior has been validated since initiation of CCoA [CN-S1-A1-3] Frequency of software/service integrity check [SI-IC-5] Software / service integrity check performed on operational systems [yes/no] [SI-IC-6]
CN-S3-A4: Validate hardware / system integrity / behavior to ensure it has not been corrupted *[Substantiated Integrity: Integrity Checks, Behavior Validation]*	Average, median, or maximum time required to validate the integrity and/or behavior of mission-critical systems or system elements [SI-ICBV-1] Percentage of mission-critical systems or system elements for which integrity / behavior has been validated since initiation of CCoA [CN-S3-A4-1] Average, median, or maximum time required to validate the integrity and/or behavior of security-critical systems or system elements [SI-ICBV-3] Percentage of security-critical systems or system elements for which integrity / behavior has been validated since initiation of CCoA [CN-S3-A4-2] Frequency of hardware / system integrity check [SI-IC-7] Hardware / system integrity check performed on operational systems [yes/no] [SI-IC-8]

B.4 Constrain

The Constrain objective – *Limit damage from adversity* – has four representative sub-objectives:

1. Identify potential damage.

2. Isolate resources to limit future or further damage.
3. Move resources to limit future or further damage.
4. Change or remove resources and how they are used to limit future or further damage.

Damage includes mission damage, cyber security damage, system damage, and damage to system elements, particularly to cyber resources.[32] These sub-objectives do not require ongoing efforts by cyber defenders (although some activities do involve such efforts), and thus apply to all types of systems. Representative activities are largely in response to detection of adverse conditions, including faults and failures.

Representative activities and metrics related to these sub-objectives are identified below.

Table 16. Constrain: Identify potential damage

Sub-Objective: Identify potential damage	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
CS-S1-A1: Identify potentially corrupted or falsified information *[Analytic Monitoring: Monitoring and Damage Assessment; Substantiated Integrity: Integrity Checks]*	Percentage of mission-critical data assets for which data integrity / quality is validated [SI-IC-2] Percentage of mission-supporting data assets for which data integrity / quality is validated [SI-IC-5] Average, minimum, or maximum time between detection or notification of a triggering event and completion of the identification / assessment process [CS-S1-A1-1] Number of locations where corrupted / falsified information checks occur Data validation includes data format, data types, and ranges [yes/no] [SI-IC-6]
CS-S1-A2: Identify potentially compromised or faulty processes or services (i.e., those which can no longer be trusted) *[Analytic Monitoring: Monitoring and Damage Assessment; Substantiated Integrity: Behavior Validation]*	Percentage of mission-critical applications for which integrity / behavior is validated [CS-S1-A2-1] Percentage of mission-supporting applications for which integrity / behavior is validated [CS-S1-A2-2] Average, minimum, or maximum time between detection or notification of a triggering event and completion of the identification / assessment process [CS-S1-A2-3] Number of locations where checks for faulty processes or services occur [SI-BV-6] Frequency of checks for faulty processes or services [continuously, on demand] [SI-BV-7]
CS-S1-A3: Identify potentially faulty, corrupted, or subverted components *[Substantiated Integrity: Integrity Checks]*	Percentage of hardware components to which tamper-evident technologies have been applied [SI-IC-9] Percentage of mission critical components that employ anti-tamper, shielding, and power line filtering [MT-115] Percentage of such components which are checked in the operational environment [CS-S1-A3-1] Frequency of checking for tamper-evidence [CS-S1-A3-2] Elapsed time between detection or notification of a triggering event and completion of the process of checking for tamper evidence [CS-S1-A3-3]

[32] As noted above, mission damage is the decrease in the ability to complete the current mission and to accomplish future missions, and may be assessed in terms of mission MOEs. System damage is the decrease in the system's ability to meet its requirements, and may be assessed in terms of system MOPs or KPPs of system elements. Damage to a system element is the decrease in that element's ability to meet its requirements, and may be assessed in terms of KPPs or other performance measures. Cyber security damage is the decrease in the ability to achieve the cyber security objectives of confidentiality, integrity, availability, and accountability, or to prevent, detect, and respond to cyber incidents; cyber security damage may be assessed in terms of cyber defense MOEs, or using cyber security metrics.

Table 17. Constrain: Isolate resources to limit future or further damage

Sub-Objective: Isolate resources to limit future or further damage	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
CS-S2-A1: Isolate an enclave or set of cyber resources suspected of being compromised or in a faulty state (e.g., to contain adversary activities, to prevent use of suspect information) *[Adaptive Response: Adaptive Management; Segmentation: Dynamic Segmentation and Isolation]*	Time between decision to isolate an enclave or a set of cyber resources and completion of isolation (latency, duration of risk exposure) [CS-S2-A1-1] Percentage or number of dynamically isolated cyber resources which can be discovered, accessed or used, or otherwise reached from some point in the network (via Red Team efforts) (a.k.a. completeness or effectiveness of isolation) [CS-S2-A1-2] Percentage or number of resources outside an isolated enclave compromised post isolation [CS-S2-A1-3]
CS-S2-A2: Isolate a critical or sensitive enclave or set of cyber resources to defend against potential compromise, faults, or failures from other resources *[Adaptive Response: Adaptive Management; Segmentation: Dynamic Segmentation and Isolation, Predefined Segmentation]*	Time between decision to isolate an enclave or a set of cyber resources and completion of isolation (latency, duration of risk exposure) [CS-S2-A1-1] Percentage or number of such isolated cyber resources which can be discovered, accessed or used, or otherwise reached from some point in the network (via Red Team efforts) (a.k.a. completeness or effectiveness of isolation) [CS-S2-A1-2] Percentage or number of resources outside an isolated enclave compromised post isolation [CS-S2-A1-3]

Table 18. Constrain: Move resources to limit future or further damage

Sub-Objective: Move resources to limit future or further damage	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
CS-S3-A1: Relocate targeted resources (e.g., physically; logically using distributed processing and virtualization) *[Dynamic Positioning: Asset Mobility, Functional Relocation of Cyber Resources]*	Percentage of resources which can be physically relocated (i.e., to another facility) [DP-AM-1] Average time to complete the physical relocation process [DP-AM-3] Percentage of resources which can be logically relocated (e.g., to a different VM) [DP-FR-1] Average time to complete the virtual relocation process [DP-FR-3]
CS-S3-A2: Dynamically relocate critical resources (e.g., physically; logically using distributed processing and virtualization) *[Dynamic Positioning: Asset Mobility, Functional Relocation of Cyber Resources]*	Percentage of critical assets which can be physically relocated (i.e., to another facility) [CS-S3-A2-1] Percentage of critical assets which can be logically relocated (e.g., to a different VM) [CS-S3-A2-2] Time to complete the relocation process for critical assets [CS-S3-A2-3]
CS-S3-A3: Reassign / relocate non-critical assets to reduce the exposure of critical assets to compromised non-critical assets *[Dynamic Positioning: Asset Mobility, Functional Relocation of Cyber Resources]*	Percentage of non-critical assets which have been analyzed with respect to the exposure they present to critical assets if compromised [CS-S3-A3-1] Percentage of non-critical assets which have been reassigned or relocated to reduce the exposure they offer to critical assets if compromised [CS-S3-A3-2] Time between decision to reassign or relocate a resource and the initial use of the relocated resource (includes time for using resources / processes to discover its new location) [CS-S3-A3-3]

Table 19. Constrain: Change or remove resources and how they are used to limit future or further damage

Sub-Objective: Change or remove resources and how they are used to limit future or further damage	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
CS-S4-A1: Recreate applications and services *[Adaptive Response: Adaptive Management; Diversity: Synthetic Diversity; Non-Persistence: Non-Persistent Services]*	Average, minimum, or maximum time between determination to recreate an application or service and discovery of resources from which it can be recreated [CS-S4-A1-1] Average, minimum, or maximum time between determination to recreate an application or service and the new instance becoming active or operational [CS-S4-A1-2] Average, minimum, or maximum time between determination to recreate an application or service and the new instance being used by other system elements [CS-S4-A1-3]
CS-S4-A2: Switch to an alternative resource *[Adaptive Response: Dynamic Reallocation; Redundancy: Replication; Unpredictability]*	Percentage of resources for which an alternative exists for which switching is performed [PA-S2-A2-1] Average time to complete the switching process (latency or lag) [PA-S2-A2-3] Average frequency of switches to an alternative resource per unit time [PA-S2-A2-4]
CS-S4-A3: Reconfigure components and services *[Adaptive Response: Dynamic Reconfiguration]*	Percentage of resources for which configuration changes can be made dynamically [PA-S2-A4-1] Percentage of resources to which configuration changes can be made randomly or in response to a triggering event [PA-S2-A4-2] Percentage of such resources for which changes are made randomly or in response to a triggering event [PA-S2-A4-3] Average time to complete the dynamic reconfiguration process (latency or lag) [PA-S2-A4-4] Frequency of configuration changes per unit time [PA-S2-A4-5]
CS-S4-A4: Dynamically relocate processing *[Adaptive Response: Dynamic Reconfiguration; Dynamic Positioning: Asset Mobility, Functional Relocation of Cyber Resources; Unpredictability]*	Percentage of resources which can be relocated virtually which are relocated [PA-S2-A5-1] Percentage of resources which can be relocated physically which are relocated [PA-S2-A5-2] Average time to complete the virtual relocation process (latency or lag) [DP-FR-3] Average time to complete the physical relocation process (latency or lag) [DP-AM-3] Frequency of relocation events per unit time [PA-S2-A5-3]
CS-S4-A5: Retain resources in an active or "live" state for a limited lifespan (e.g., maximum time period after instantiation or creation, maximum period after use) *[Non-Persistence: Non-Persistent Services, Non-Persistent Connectivity, Non-Persistent Information]*	Maximum or average lifespan of a communications path [PA-S2-A6-6] Maximum or average lifespan of a mission service [PA-S2-A6-7] Maximum or average lifespan of a supporting service [PA-S2-A6-8] Maximum or average lifespan of an information resource [PA-S2-A6-9]

Sub-Objective: Change or remove resources and how they are used to limit future or further damage	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
CS-S4-A6: Ensure that termination, deletion, or movement does not leave residual mission-critical or sensitive data or software behind *[Dynamic Positioning: Functional Relocation of Cyber Resources; Non-Persistence: Non-Persistent Services, Non-Persistent Connectivity]*	Amount of [mission critical, sensitive] information which can be retrieved or reconstructed by a Red Team after a service is moved or terminated (as percentage of amount of information which can be obtained by a Red Team if the service is not moved or terminated) [PA-S2-A7-1] Amount of information which can be retrieved or reconstructed by a Red Team after an information resource is deleted (as a percentage of amount of information in the resource prior to deletion) [PA-S2-A7-2]
CS-S4-A7: Modify privilege restrictions *[Privilege Restriction: Dynamic Privileges; Unpredictability: Temporal Unpredictability, Contextual Unpredictability]*	Percentage of cyber resources for which privileges can be modified dynamically [PV-DP-1] Percentage of such users whose privileges are modified randomly or as part of a CCoA [CS-S4-A7-1] Percentage of users for whom privileges can be modified dynamically [PV-DP-2] Percentage of such users whose privileges are modified randomly or as part of a CCoA [CS-S4-A7-2] Percentage of system services for which privileges can be modified randomly [PV-DP-3] Percentage of such resources for which privileges are modified randomly or as part of a CCoA [CS-S4-A7-3]

B.5 Reconstitute

The Reconstitute objective – *Restore as much mission or business functionality as possible subsequent to adversity* – has four representative sub-objectives:

1. Identify damage and untrustworthy resources. Damage need not be identified with specific resources; for example, degraded service can be systemic. Resources (e.g., processes) can be untrustworthy even if they appear to be performing correctly.
2. Restore functionality.
3. Heighten protections during reconstitution.
4. Determine the trustworthiness of restored or reconstructed resources.

The first two sub-objectives do not require ongoing efforts by cyber defenders (although some activities do involve such efforts), and thus apply to all types of systems. The last two sub-objectives do strongly involve cyber defender efforts, and thus are not representative of unfederated CPS or of PIT operating in stand-off mode.

Representative activities and metrics related to these sub-objectives are identified below.

Table 20. Reconstitute: Identify damage and untrustworthy resources

Sub-Objective: Identify damage and untrustworthy resources	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
RE-S1-A1: Identify resources that have been destroyed, damaged beyond repair, or otherwise made unavailable (e.g., network connections lost) *[Analytic Monitoring: Monitoring and Damage Assessment; Contextual Awareness: Mission Dependency and Status Visualization]*	Time to identify unavailable resources and represent damage in status visualization [RE-S1-A1-1] Time to notify services or mission / business functions which use damaged or unavailable resources that those resources are no longer available [RE-S1-A1-2]
RE-S1-A2: Identify corrupted, falsified, or suspect information *[Analytic Monitoring: Monitoring and Damage Assessment; Substantiated Integrity: Integrity Checks]*	Percentage of mission-critical data assets for which data integrity / quality is validated [SI-IC-2] Percentage of mission-supporting data assets for which data integrity / quality is validated [SI-IC-5] Average, minimum, or maximum time to identify suspect information [RE-S1-A1-1] Number of locations where corrupted / falsified information checks occur [CS-S1-A1-2] Data validation includes data format, data types, and ranges [yes/no] [SI-IC-6] Time to notify services or mission / business functions which use suspect information to delete or disregard that information [RE-S1-A1-2]
RE-S1-A3: Identify compromised, faulty, or suspect processes or services (i.e., those which can no longer be trusted) *[Analytic Monitoring: Monitoring and Damage Assessment; Substantiated Integrity: Behavior Validation]*	Percentage of [mission-critical, security-critical, supporting] processes or services which are validated [RE-S1-A3-1] Time to identify suspect [mission-critical, security-critical, supporting] processes or services [RE-S1-A3-2] Time to notify services or mission / business functions which use or communicate with suspect processes or services to terminate interactions with those services [RE-S1-A3-3]
RE-S1-A4: Identify damaged, corrupted, or subverted components *[Substantiated Integrity: Integrity Checks]*	Percentage of hardware components to which tamper-evident technologies have been applied [SI-IC-9] Percentage of mission critical components that employ anti-tamper, shielding, and power line filtering [MT-115] Percentage of such components which are checked [RE-S1-A4-1] Time to identify damaged components [RE-S1-A4-2]

Table 21. Reconstitute: Restore functionality

Sub-Objective: Restore functionality	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
RE-S2-A1: Execute recovery procedures in accordance with contingency or continuity of operations plans *[Coordinated Protection: Orchestration; Redundancy: Protected Backup and Restore]*	Time between initiation of recovery procedures and completion of documented milestones in the recovery, contingency, or continuity of operations plan [MT-37] Time between event or detected circumstances which motivated recovery procedures and achievement of [minimum acceptable, target] mission MOPs [MT-20] Percentage of mission capabilities for which [minimum acceptable, target] MOPs are achieved within [minimum threshold, target] period of time since initiating event [RE-S2-A1-1] Percentage of mission-critical cyber resources which are recovered from a backup [RE-S2-A1-2] Size of gap between lost and recovered mission-critical resources (time service or connection was unavailable, number of records not recovered) [RE-S2-A1-3] Percentage of mission-essential processes and interfaces restored to pre-disruption state [MT-89] Length of time to reconstitute a key information asset from a backup data store [MT-184]
RE-S2-A2: Restore non-critical functional capabilities *[Adaptive Response: Dynamic Reconfiguration, Dynamic Resource Allocation; Redundancy: Protected Backup and Restore]*	Time between event or detected circumstances which motivated recovery procedures and achievement of [minimum acceptable, target] MOPs for supporting functional capabilities [RE-S2-A2-1] Percentage of supporting functional capabilities for which [minimum acceptable, target] MOPs are achieved within [minimum threshold, target] period of time since initiating event [RE-S2-A2-2] Percentage of non-mission-critical resources which are recovered from a backup [RE-S2-A2-3] Size of gap between lost and recovered non-mission-critical resources (time service or connection was unavailable, number of records not recovered) [RE-S2-A2-4]
RE-S2-A3: Coordinate recovery activities to avoid gaps in security coverage *[Adaptive Response: Adaptive Management; Analytic Monitoring: Monitoring and Damage Assessment; Coordinated Protection: Orchestration, Calibrated Defense-in-Depth; Dynamic Positioning: Functional Relocation of Sensors; Contextual Awareness: Mission Dependency and Status Visualization; Privilege Restriction: Attribute-Based Usage Restrictions]*	Percentage of cyber resources for which access control is maintained throughout the recovery process [RE-S2-A3-1] Percentage of cyber resources for which access controls at multiple levels or using different mechanisms are maintained consistently throughout the recovery process [RE-S2-A3-2] Percentage of cyber resources for which auditing or monitoring is maintained throughout the recovery process [RE-S2-A3-3] Duration of gap in auditing or monitoring for [mission-critical resource, non-mission-critical resource] during recovery [RE-S2-A3-4]

Sub-Objective: Restore functionality	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
RE-S2-A4: Reconstruct compromised (i.e., destroyed, corrupted) critical assets or capabilities from existing resources *[Adaptive Response: Dynamic Reconfiguration; Coordinated Protection: Orchestration; Dynamic Positioning: Fragmentation, Distributed Functionality]*	Percentage of compromised critical information stores which are reconstructed from existing resources [RE-S2-A4-1] Percentage of compromised critical information stores which are irretrievably lost [RE-S2-A4-2] Percentage of compromised services or functions which are reconstructed from existing resources [RE-S2-A4-3] Time to reconstruct an asset or capability from existing resources [RE-S2-A4-4] Time to reconstruct an asset or capability from the current gold image [RE-S2-A4-5] Time to reconstruct an asset or capability from a previous gold image [RE-S2-A4-6] Minimum amount of information or service loss necessary to make the system inoperable [RE-S2-A4-7] Time to locate tools, services, and data sources needed to repair or reconstitute an infrastructure that serves mission requirements [MT-189] Time to combine tools, services, and data sources needed to repair or reconstitute the infrastructure that serves mission requirements [MT-192} 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 [MT-195]

Table 22. Reconstitute: Heighten protections during reconstitution

Sub-Objective: Heighten protections during reconstitution	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
RE-S3-A1: Intensify monitoring of restored or reconstructed resources *[Adaptive Response: Adaptive Management; Dynamic Positioning: Functional Relocation of Sensors]*	Percentage of cyber resources for which additional auditing or monitoring is applied during and after the recovery process [RE-S3-A1-1] Length of time to bring online a backup network intrusion detection system [MT-132]
RE-S3-A2: Isolate or restrict access to or by restored or reconstructed resources *[Coordinated Protection: Orchestration; Privilege Restriction: Dynamic Privileges, Attribute-Based Usage Restriction; Segmentation: Predefined Segmentation, Dynamic Segmentation and Isolation]*	Percentage of reconstituted cyber resources for which more stringent access controls are applied during and after reconstitution [RE-S3-A2-1] Percentage of reconstituted cyber resources which are placed in a restricted enclave for a period after reconstitution [RE-S3-A2-2]

Table 23. Reconstitute: Determine the trustworthiness of restored or reconstructed resources

Sub-Objective: Determine the trustworthiness of restored or reconstructed resources	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
RE-S4-A1: Validate data provenance of restored or reconstructed resources *[Substantiated Integrity: Provenance Tracking]*	Percentage of restored or reconstructed [mission-critical, security-critical, supporting] data assets for which data provenance is validated [RE-S4-A1-1]

Sub-Objective: Determine the trustworthiness of restored or reconstructed resources	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
RE-S4-A2: Validate data integrity / quality of restored or reconstructed resources to ensure they not been corrupted *[Substantiated Integrity: Integrity Checks]*	Percentage of restored or reconstructed [mission-critical, security-critical, supporting] data assets for which data integrity / quality is checked [RE-S3-A2-1] Quality of restored / recovered / reconstituted data [MT-22]
RE-S4-A3: Validate software / service integrity / behavior of restored or reconstructed applications, services, and processes to ensure they have not been corrupted *[Substantiated Integrity: Behavior Validation]*	Percentage of restored or reconstructed [mission-critical, security-critical, supporting] applications, services, and processes for which behavior is checked [RE-S4-A2-1]
RE-S4-A4: General	Level of trust in a system that has been restored to its pre-disruption capability [MT-90]

B.6 Understand

The Understand objective – Maintain useful representations of mission and business dependencies and the status of resources with respect to possible adversity – has four representative sub-objectives:

1. Understand adversaries.
2. Understand dependencies on and among cyber resources. Note that the activities supporting this sub-objective assume implementation of the subcategories of the Asset Management category of activities, under the Identify function in the CSF Framework Core.
3. Understand the status of resources with respect to threat events.
4. Understand the effectiveness of cyber security and cyber resiliency controls.

The first sub-objective is meaningful when cyber defenders are part of the system, and thus is not representative of unfederated CPS or of PIT operating in stand-off mode; the second is meaningful when human operators and/or cyber defenders are part of the system, and thus may not be representative of such systems. However, some activities under these sub-objectives may executable by automation emulating defensive or operational decision-making.

Representative activities and metrics related to these sub-objectives are identified below.

Table 24. Understand: Understand adversaries

Sub-Objective: Understand adversaries	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
UN-S1-A1: Use shared threat information *[Analytic Monitoring: Sensor Fusion and Analysis; Contextual Awareness: Dynamic Threat Awareness]*	Number of threat information feeds the organization uses [UN-S1-A1-1] Frequency with which receipt of threat information is updated [UN-S1-A1-2] Time between receipt of threat intelligence and determination of its relevance [UN-S1-A1-3] Time between determination that threat intelligence is relevant and promulgation of defensive TTPs [UN-S1-A1-4] Frequency with which the organization provides threat information to the broader community [UN-S1-A1-5] Number of threat types/communities the organization monitors [UN-S1-A1-6]
UN-S1-A2: Reveal adversary TTPs by analysis *[Analytic Monitoring: Malware and Forensic Analysis]*	Time between initiation of malware or forensic analysis and use or sharing of results of analysis [UN-S1-A2-1] Average number per campaign or intrusion set of indicators or observables developed by self-analysis of malware or other artifacts [UN-S1-A2-1]
UN-S1-A3: Observe and analyze adversary activities in deception environments (e.g., honeypots, honeynets, decoy documents or data stores) *[Deception: Misdirection; Analytic Monitoring: Sensor Fusion and Analysis; Contextual Awareness: Dynamic Threat Awareness]*	Number of deception environments provided [UN-S1-A3-1] Representativeness of deception environment – size [ratio of number of cyber resources in deception enclave to number of cyber resources in real enclave] [UN-S1-A2-2] Percentage of enclaves providing deception [UN-S1-A2-3] Number of attempted intrusions deflected to a honeypot [MT-4] Adversary dwell time in deception environment [MT-264] Percentage of attackers in a deception environment who are unaware of their containment [MT-265] Percentage of times attacker goals can be discerned from activities in a deception environment [MT-266] Percentage of times an attacker in a deception environment closes out their encounter normally (i.e., removes traces of activity) [MT-267] Number of observables or indicators developed per adversary engagement [UN-S1-A2-4] Average number of subsequent accesses by an adversary to a deception environment [UN-S1-A2-5] Number of times the adversary has positively identified/recognized the deception environment [UN-S1-A2-6]
UN-S1-A4: Reveal adversary data collection or exfiltration *[Deception: Tainting]*	Percentage of high-value information assets which include hidden beaconing functionality [UN-S1-A4-1] Percentage of high-value information assets which include hidden signatures which make them discoverable via network searches [UN-S1-A4-2]

Table 25. Understand: Understand dependencies on and among cyber resources

Sub-Objective: Understand dependencies on and among cyber resources	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
UN-S2-A1: Perform impact analysis[33] to identify critical assets / capabilities *[Coordinated Protection: Consistency Analysis; Contextual Awareness: Dynamic Resource Awareness]*	Time since most recent update of MIA, BIA, or CJA [UN-S2-A1-1] Extent of validation of MIA, BIA, or CJA (e.g., review, tabletop exercise, COOP exercise) [UN-S2-A1-2] Percentage of cyber resources for which criticality has been determined [UN-S2-A1-3]
UN-S2-A2: Identify, and maintain a representation of, mission dependencies on cyber resources *[Contextual Awareness: Dynamic Resource Awareness]*	Time required to refresh mission dependency map [112] [113] [30] [UN-S2-A2-1] Time since most recent refresh of mission dependency map [UN-S2-A2-2] Degree of completeness of mission dependency map [UN-S2-A2-3] Percent of known cyber resources included in mission dependency map [UN-S2-A2-4]
UN-S2-A3: Identify, and maintain a representation of, functional dependencies among cyber resources[34] *[Contextual Awareness: Dynamic Resource Awareness]*	Time required to refresh functional dependency map [30] [UN-S2-A3-1] Time since most recent refresh of functional dependency map [UN-S2-A3-2] Degree of completeness of functional dependency map [UN-S2-A3-3] Percent of known cyber resources included in functional dependency map [UN-S2-A3-4]
UN-S2-A4: Identify, and maintain a representation of, functional dependencies on external resources[35] *[Contextual Awareness: Dynamic Resource Awareness]*	Time required to refresh external dependency map or inventory [UN-S2-A4-1] Time since most recent refresh of external dependency map or inventory [UN-S2-A4-2] Degree of completeness of external dependency map or inventory [UN-S2-A4-3]
UN-S2-A5: Validate assumptions about dependencies and criticality by controlled disruption[36] *[Coordinated Protection: Self-Challenge]*	Time since last cyber table-top exercise, Red Team exercise, or execution of controlled automated disruption (e.g., via Simian Army) [UN-S2-A5-1] Frequency of cyber table-top exercises, Red Team exercises, or execution of controlled automated disruption [UN-S2-A5-1] Percentage of red team attack scenarios where varying configurations of interrelated functions are subjected to attack [MT-101]
UN-S2-A6: Determine types and degrees of trust for users and cyber entities (e.g., components, data, processes, interfaces) *[Coordinated Protection: Consistency Analysis]*	Number of types of users for which degrees of trust are defined [UN-S2-A6-1] Number of types of cyber entities for which degrees of trust are defined [UN-S2-A6-2]

[33] Examples include mission impact analysis (MIA) [30], business impact analysis (BIA) as defined in NIST SP 800-34R1 [157] and crown jewels analysis (CJA) [110]. This activity is typically performed in support of continuity of operations (COOP) planning.

[34] Functional dependencies and mission dependencies can be identified and represented simultaneously in most architectures. However, functional dependencies can be identified without insight into mission processes, e.g., by a cloud service provider.

[35] External resources are those not under the control of the system operator, e.g., electrical power (if the system or mission is not related to electrical power provision).

[36] A controlled disruption is a disruption intentionally caused by the system operator or cyber defender, in order to identify weaknesses or single points of failure. Examples include the Simian Army (https://github.com/Netflix/SimianArmy/wiki) for cloud services, Red Team exercises, and large-scale cyber wargames [158].

Table 26. Understand: Understand the status of resources with respect to threat events

Sub-Objective: Understand the status of resources with respect to threat events	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
UN-S3-A1: Track security posture of cyber resources (e.g., patch status, compliance with configuration guidance, distance to alert thresholds) *[Analytic Monitoring: Monitoring and Damage Assessment]*	[Many FISMA and CDM metrics can be repurposed.] Percentage of cyber resources that are properly configured [MT-1] Frequency of audit record analysis for inappropriate activity [MT-42] Percentage of systems for which a defined security configuration is required [MT-62] Length of time for detailed information about a system to be delivered to an operator who has requested it in response to an alert [MT-160] Length of time to report packets to/from an invalid port on a server [MT-176] Length of time to report attempts to access unauthorized ports or inaccessible addresses [MT-177] Length of time to report attempts at IP address spoofing [MT-178] Length of time for packets to unroutable IP addresses to be reported [MT-179] Length of time for packets to/from an invalid port on a server to be reported [MT-180]
UN-S3-A2: Coordinate sensor coverage to minimize gaps or blind spots *[Analytic Monitoring: Sensor Fusion and Analysis; Coordinated Protection: Orchestration]*	Percentage of cyber resources monitored [UN-S3-A2-1] Percentage of types of cyber resources monitored [UN-S3-A2-2]
UN-S3-A3: Coordinate sensor coverage to mitigate adversary's attempts to thwart monitoring *[Analytic Monitoring: Monitoring and Damage Assessment; Coordinated Protection: Orchestration; Deception: Obfuscation]*	Percentage of Network Intrusion Detection Systems that are connected to the network using passive taps [MT-127] Percentage of Network Intrusion Detection Systems that use an out-of-band network for remote management [MT-129] Number or percentage of Network Intrusion Detection Systems that are implemented on separate platforms [MT-131] Length of time packet capture and sniffing devices are connected to the network [MT-133]
UN-S3-A4: Correlate or otherwise combine data from different sensors *[Analytic Monitoring: Sensor Fusion and Analysis]*	Percentage of those cyber resources monitored by more than one sensor [UN-S3-A4-1] Number or percentage of sensors from which data is correlated or fused with data from other sensors [UN-S3-A4-2]
UN-S3-A5: Develop custom analytics or sensors *[Analytic Monitoring: Monitoring and Damage Assessment]*	Percentage of cyber resources for which custom analytics have been developed [UN-S3-A5-1]
UN-S3-A6: Dynamically reconfigure sensors *[Adaptive Response: Dynamic Reconfiguration]*	Elapsed time for sensor reconfiguration to take effect [UN-S3-A6-14] Percentage of sensors capable of being reconfigured [UN-S3-A6-2]
UN-S3-A7: Perform damage assessment *[Analytic Monitoring: Monitoring and Damage Assessment; Substantiated Integrity: Integrity Checks, Behavior Validation]*	Percentage of system elements for which failure or indication of potential faults can be detected [UN-S3-A7-1] Percentage of cyber resources for which damage can be assessed [UN-S3-A7-2] Elapsed time for damage assessment [AM-DA-1]

Sub-Objective: Understand the status of resources with respect to threat events	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
UN-S3-A8: Search externally for evidence of exfiltrated data *[Analytic Monitoring: Monitoring and Damage Assessment; Deception: Tainting]*	Time since last external search [UN-S3-A8-1] Number of external locations on which exfiltrated data are found [UN-S3-A8-2]
UN-S3-A9: Dynamically relocate sensors *[Dynamic Positioning: Functional Relocation of Sensors]*	Elapsed time between decision to relocate a sensor and delivery of initial sensor data [UN-S3-A9-1]
UN-S3-A10: Define and maintain a representation of the resiliency posture[37] of cyber resources and adversary activities against cyber resources *[Contextual Awareness: Mission Dependency and Status Visualization]*	Time to refresh the representation of the resiliency posture [UN-S3-A10-1] Percentage of critical resources represented in posture [UN-S3-A10-2] Percentage of system resources represented in the resiliency posture representation [UN-S3-A10-3]
UN-S3-A11: Validate provenance and quality of hardware and software *[Substantiated Integrity: Provenance Tracking]*	Percentage of mission-critical hardware components for which supply chain and assurance evidence is maintained [UN-S3-A11-1] Percentage of mission-critical software components for which supply chain and assurance evidence is maintained [UN-S3-A11-2]
UN-S3-A12: Validate data provenance *[Substantiated Integrity: Provenance Tracking]*	Percentage of mission-critical data assets for which data provenance measures have been implemented [UN-S3-A12-1] Percentage of mission-critical data assets for which data provenance has been validated in the last [specify time period; will depend on mission tempo] [UN-S3-A12-2]
UN-S3-A13: Validate data integrity / quality to ensure it has not been corrupted *[Substantiated Integrity: Integrity Checks]*	Percentage of mission-critical data assets for which data integrity / quality has been validated in the last [specify time period; will depend on mission tempo] [UN-S3-A13-1] Percentage of mission-supporting[38] data assets for which data integrity / quality has been validated in the last [specify time period; will depend on mission tempo] [UN-S3-A13-2] Percentage of unauthorized changes to row data in a database that are detected [MT-181]
UN-S3-A14: Validate software / service integrity / behavior to ensure it has not been corrupted *[Substantiated Integrity: Integrity Checks, Behavior Validation]*	Percentage of mission-critical applications for which integrity / behavior has been validated in the last [specify time period; will depend on mission tempo] [UN-S3-A14-1] Percentage of mission-supporting[39] services for which integrity / behavior has been validated in the last [specify time period; will depend on mission tempo] [UN-S3-A14-2] Frequency of software / service integrity check [UN-S3-A14-3] Percentage of security components that are monitored for communication between an adversary and their implanted malicious code [MT-114]
UN-S3-A15: Validate component integrity *[Substantiated Integrity: Provenance Tracking]*	Percentage of hardware components for which provenance can be tracked [UN-S3-A15-1] Percentage of hardware components for which provenance actually is tracked [UN-S3-A15-2]

[37] A system's resiliency posture can include its security posture, its performance with respect to SLAs or KPPs, and the quality of key resources as determined using Substantiated Integrity mechanisms.
[38] Note that mission-supporting data assets can include those which security-critical.
[39] Note that mission-supporting services can include those which are security-critical.

Table 27. Understand: Understand the effectiveness of cyber security and cyber resiliency controls

Sub-Objective: Understand the effectiveness of cyber security and cyber resiliency controls	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
UN-S4-A1: Track effectiveness of defenses at different architectural locations *[Analytic Monitoring: Monitoring and Damage Assessment]*	Number of attempted intrusions stopped at a network perimeter [MT-2] Number of attempted intrusions deflected to a honeypot [MT-4] Percentage of systems in compliance with organizationally mandated configuration guidance [MT-39] Average length of time between cyber incidents [MT-49]
UN-S4-A2: Track effectiveness of detection mechanisms at different architectural locations *[Analytic Monitoring: Monitoring and Damage Assessment, Malware and Forensic Analysis]*	Length of time between an initial adversary act and its detection [MT-6] Average length of time between the start of adversary activities and their discovery [MT-35] Average length of time between the occurrence and the discovery of an anomaly [MT-47] Percentage of managed systems checked for vulnerabilities in accordance with the organization's policy [MT-55] Percentage of enterprise considered to be monitored effectively [MT-65] Percentage of classes of attacks that can be detected with existing means [MT-83]
UN-S4-A3: Track effectiveness of CCoAs *[Adaptive Response: Adaptive Management; Coordinated Protection: Consistency Analysis, Orchestration]*	Additional / diverted level of effort to maintain mission-essential functions for a given CCoA [MT-10] Percentage of data irrevocably lost due to an incident [MT-24] Average length of time to recover from incidents [MT-37] Percentage of incidents reported within required timeframe per applicable incident category [MT-46] Average length of time for the organization to recover from damage caused by a cyber incident [MT-53]

B.7 Transform

The Transform objective – Modify mission or business functions and supporting processes to handle adversity and address environmental changes more effectively – has two representative sub-objectives:

1. Redefine mission threads for agility.
2. Redefine mission / business functions to mitigate risks.

More meaningful and useful sub-objectives and activities for this objective can be defined in the context of a specific use case. Both these sub-objectives, and the Transform objective as a whole, assume active human participation – by mission or business function owners, by system operators or users, and (to the extent that cyber defense is part of mission operations) cyber defenders – in activities which are not part of system operations.

Representative activities and metrics related to these sub-objectives are identified below.

Table 28. Transform: Redefine mission threads for agility

Sub-Objective: Redefine mission threads for agility	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
TR-S1-A1: Identify and eliminate single points of failure in mission threads *[Redundancy: Replication; Coordinated Protection: Consistency Analysis, Orchestration]*	Percentage of mission threads which have been analyzed with respect to common dependencies and potential single points of failure [TR-S1-A1-1] Percentage of mission threads for which no single points of failure can be identified [TR-S1-A1-1]
TR-S1-A2: Identify and resource alternative mission courses of action *[Coordinated Protection: Consistency Analysis, Orchestration]*	Percentage of mission threads for which alternative courses of action are documented [TR-S1-A2-1] Percentage of staff identified in documented alternative courses of action who have been trained in those alternatives [TR-S1-A2-2]
TR-S1-A3: Reduce the overhead and risk associated with persistent processing or communications *[Non-Persistence: Non-Persistent Services, Non-Persistent Communications]*	Percentage of services or processes which have been made non-persistent [TR-S1-A3-1] Percentage of services or processes for which connectivity is established on-demand and dropped after transaction completion [TR-S1-A3-2] Percentage of ports / protocols for which use is enabled on-demand and dropped after transaction completion[TR-S1-A3-3]

Table 29. Transform: Redefine mission / business functions to mitigate risks

Sub-Objective: Redefine mission / business functions to mitigate risks	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
TR-S2-A1: Identify and mitigate unnecessary dependencies of mission threads on resources shared with non-mission functions *[Realignment: Purposing]*	Percentage of mission threads for which no dependencies on resources shared with non-mission functions can be identified [TR-S2-A1-1] Percentage of mission threads for which risk remediation of dependencies on resources shared with non-mission functions is represented in CCoA(s) or cyber playbook [TR-S2-A1-2]
TR-S2-A2: Reallocate resources and/or reassign administrative / management responsibility based on risk to mission / business function *[Realignment: Restriction, Offloading; Coordinated Protection: Consistency Analysis, Orchestration]*	Percentage of resources for which privilege requirements have been analyzed with respect to risk-benefit trade-offs [TR-S2-A2-1] Percentage of problematic privilege assignments which have been changed since last analysis [TR-S2-A2-2]
TR-S2-A3: Identify and remove or replace data feeds and connections for which risks outweigh benefits *[Realignment: Restriction, Offloading]*	Percentage of data feeds which have been analyzed (e.g., in terms of sources and protocols) with respect to risk-benefit trade-offs [TR-S2-A3-1] Percentage of problematic data feeds to which risk mitigations have been applied since last analysis [TR-S2-A3-3]
TR-S2-A4: Identify and remove or replace components for which risks outweigh benefits *[Realignment: Specialization, Replacement]*	Percentage of components which have been analyzed (e.g., in terms of supply chain or privilege requirements) with respect to risk-benefit trade-offs [TR-S2-A4-1] Percentage of problematic components to which risk mitigations have been applied since last analysis [TR-S2-A4-2]
TR-S2-A5: Analyze data to assess lifespan / retention conditions and apply automated deletion / obfuscation *[Non-Persistence: Non-Persistent Information]*	Percentage of data stores for which automated deletion / obfuscation has been implemented [TR-S2-A5-1] Percentage of data stores for which lifespan / retention conditions have been analyzed [TR-S2-A5-2]

B.8 Re-Architect

The Re-Architect objective – *Modify architectures to handle adversity and address environmental changes more effectively* – has two representative sub-objectives:

1. Restructure systems or sub-systems to reduce risks.
2. Modify systems or sub-systems to reduce risks.

More meaningful and useful sub-objectives and activities for this objective can be defined in the context of a specific use case. Both these sub-objectives, and the Re-Architect objective as a whole, assume active human participation – by mission or business function owners and by systems engineers – in activities which are not part of system operations.

Representative activities and metrics related to these sub-objectives are identified below.

Table 30. Re-Architect: Restructure systems or sub-systems to reduce risks

Sub-Objective: Restructure systems or sub-systems to reduce risks	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
RA-S1-A1: Restructure systems or sub-systems to minimize the number of critical assets *[Realignment: Purposing, Restriction]*	Percentage of cyber resources identified as critical assets (compared with same value at previous times or for prior spirals) [RA-S1-A1-1]
RA-S1-A2: Restructure systems, sub-systems, or workflows to reduce the duration of exposures *[Non-Persistence: Non-Persistent Information, Non-Persistent Services, Non-Persistent Connectivity]*	Percentage of cyber resources which are non-persistent (compared with same value at previous times or for prior spirals) [RA-S1-A2-1]
RA-S1-A3: Restructure systems or sub-systems to maximize agility in the face of potential changes in missions and mission processes, business functions and offerings, and disruptive technologies *[Coordinated Protection: Consistency Analysis, Orchestration; Realignment: Specialization, Replacement, Offloading]*	Percentage of systems or sub-systems which can be repurposed or recomposed [RA-S1-A3-1]

Sub-Objective: Restructure systems or sub-systems to reduce risks	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
RA-S1-A4: Restructure systems or sub-systems to improve defensibility in the face of predicted long-term changes in adversary capabilities, intent, and/or targeting *[Realignment: Specialization, Replacement, Offloading, Restriction; Segmentation: Predefined Segmentation]*	Size of the hardware attack surface (e.g., computed as function of the number of device types and the number of devices of each type; for an individual device, computed as a function of the types and numbers of physical communications ports, and the number and types of ports and protocols [114] [115]) [RA-S1-A4-1] Size of the software attack surface (using a well-defined method, e.g., [116]) [RA-S1-A4-2] Size of the supply chain attack surface (e.g., number of organizations in the supply chain for a given critical component, number of organizations in the supply chain for all components) (using a well-defined method, e.g., [116]) (e.g., number of organizations in the supply chain for a given critical component, number of organizations in the supply chain for all components) [RA-S1-A4-3] Size of the general user attack surface [RA-S1-A4-4] Size of the privileged user attack surface [RA-S1-A4-5] Percentage of system components for which provenance can be determined [RA-S1-A4-6] Percentage of critical system components for which provenance can be determined [RA-S1-A4-7] Percentage of system components which can be selectively isolated [RA-S1-A4-8]

Table 31. Re-Architect: Modify systems or sub-systems to reduce risks

Sub-Objective: Modify systems or sub-systems to reduce risks	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
RA-S2-A1: Identify and mitigate unnecessary dependencies of mission threads on resources shared with non-mission functions *[Realignment: Purposing]*	Percentage of mission threads for which no dependencies on resources shared with non-mission functions can be identified [RA-S2-A1-1] Percentage of mission threads for which risk remediation of dependencies on resources shared with non-mission functions is represented in CCoA(s) or cyber playbook [RA-S2-A1-2]
RA-S2-A2: Reallocate resources and/or reassign administrative / management responsibility based on risk to mission / business function *[Realignment: Restriction, Offloading; Coordinated Protection: Consistency Analysis, Orchestration]*	Percentage of resources for which privilege requirements have been analyzed with respect to risk-benefit trade-offs [RA-S2-A2-1] Percentage of problematic privilege assignments which have been changed since last analysis [RA-S2-A2-2]
RA-S2-A3: Identify and remove or replace data feeds and connections for which risks outweigh benefits *[Realignment: Restriction, Offloading]*	Percentage of data feeds and connections which have been analyzed (e.g., in terms of sources and protocols) with respect to risk-benefit trade-offs (e.g., connection supports a service which has been retired) [RA-S2-A3-1] Percentage of problematic data feeds and connections to which risk mitigations have been applied since last analysis [RA-S2-A3-2]
RA-S2-A4: Identify and remove or replace components for which risks outweigh benefits *[Realignment: Specialization, Replacement]*	Percentage of components which have been analyzed (e.g., in terms of supply chain or privilege requirements) with respect to risk-benefit trade-offs [RA-S2-A4-1] Percentage of problematic components to which risk mitigations have been applied since last analysis [RA-S2-A4-2] Percentage of sub-systems or components redesigned to improve damage limitation [MT-26]

Sub-Objective: Modify systems or sub-systems to reduce risks	
Representative Activity and *Corresponding Approaches*	**Possible Representative Metrics and Measures**
RA-S2-A5: Analyze data to assess lifespan / retention conditions and apply automated deletion / obfuscation *[Non-Persistence: Non-Persistent Information]*	Percentage of data stores for which automated deletion / obfuscation has been implemented [RA-S2-A5-1] Percentage of data stores for which lifespan / retention conditions have been analyzed [RA-S2-A5-2]
RA-S2-A6: Develop custom analytics or sensors *[Analytic Monitoring: Monitoring and Damage Assessment]*	Percentage of cyber resources for which custom analytics have been developed [RA-S2-A6-1] Number of new sensors installed [MT-27]
RA-S2-A7: Re-implement critical components to reduce risks and provide alternative implementations (which may be swapped in at a defender-chosen time) *[Diversity: Design Diversity, Synthetic Diversity, Path Diversity, Supply Chain Diversity; Realignment: Specialization, Replacement]*	Percentage of mission critical components that are purpose built [MT-117] Percentage of mission-critical components for which one or more custom-built alternatives are implemented [RA-S2-A7-1] Percentage of mission-critical components for which one or more alternative sources are available [RA-S2-A7-1] Length of time to deploy a new instantiation of a required capability [MT-31]
RA-S2-A8: Create and maintain a demonstrably different version of the system or of critical sub-systems *[Diversity: Architectural Diversity, Design Diversity, Information Diversity, Path Diversity, Supply Chain Diversity; Redundancy: Replication]*	Number of different technical architecture standards for the same or similar capabilities used [RA-S2-A8-1] Percentage of critical data stores for which alternatives derived from different data sources are maintained [RA-S2-A8-2] Percentage of system resources for which alternatives from non-overlapping supply chains are maintained [RA-S2-A8-3]
RA-S2-A9: General	Percentage of individually managed systems in which one or more resiliency techniques have been implemented [MT-86]

Appendix C Cyber Resiliency Metric Template

This Appendix presents a template that organizations can use to specify metrics in enough detail that their intended uses are clear. Template elements which are underlined are captured in the Cyber Resiliency Metrics Catalog, and are discussed in more detail in the report which describes the catalog [11].

Table 32. Cyber Resiliency Metric Template

Template Element	Description and *Guidance*
Identification *These fields must always be populated.*	
Metric Name/ Identifier	Name or identifier of base metric. *Guidance: Make the identifier short but unique.*
Descriptor	Provide a short description of what being measured. *Guidance: Make the description succinct but clear. The description should suggest the form of the metric (e.g., percentage, time, degree).*
Cyber Resiliency Properties Being Measured *If none of these fields can be populated, the metric cannot be claimed as a cyber resiliency metric. (It may still serve as a measure of performance, changes in which constitute a measure of effectiveness for a cyber resiliency solution.)*	
Cyber Resiliency Goal(s) and Goal-Related Question(s)	Identify the relevant goal or goals for which this metric either provides a direct measure or answers a relevant question. If possible, identify the motivating question or questions the metric can be used to answer, to help reduce the potential for misinterpretation. Format: "Goal" (separated by commas, if multiple goals); new paragraph for discussion *Guidance: Examples of questions include* • *Anticipate: How well prepared are we to counter low-level disruptions?* • *Withstand: How well do perimeter defenses withstand attack? How well can mission operations withstand the loss of cyber resources?* • *Recover: How quickly can mission-essential functionality be restored to its minimum required level?* • *Adapt: How quickly can the system change to continue to meet mission needs?* *The question(s) should be made more specific for a tailored version of the metric, e.g., by identifying specific missions, functions, sub-organizations, assets, or resources.* *The discussion can also include (or reference) a description of, or a set of anchoring examples for, the meaning of each identified goal in the context of the organization, program, or system for which the metric is defined.*
Cyber Resiliency Objective(s) and Objective-Related Question(s)	Identify the cyber resiliency objective(s) for which this metric either provides a direct measure, serves as an indicator of achievement, or answers a relevant question. If possible, identify the motivating question or questions the metric can be used to answer, to help reduce the potential for misinterpretation. If necessary, provide the relevant restatement of Format: "Objective" or "Objective: Question" separated by commas; new paragraph for discussion. *Guidance: The discussion can include questions, and can also include the meaning or interpretation of the relevant objective(s).* *Questions: In many cases, a goal-related question will be identical to an objective-related question. In general, questions take the form "how well is a representative sub-objective achieved?" (with the corresponding metric being a measure of completeness or effectiveness, where effectiveness can have a temporal aspect) or "how quickly can an activity which supports or demonstrates achieving the objective be performed?" (with the corresponding metric being a measure of timeliness). Examples include* • *Prevent / Avoid: How well does the organization create and maintain deception environments?* • *Prepare: How completely does the organization back up data needed to restore or reconstitute mission and supporting functionality?*

Template Element	Description and *Guidance*
	• *Continue: How well does the system validate the correctness of its mission-essential functions?* • *Constrain: How quickly can critical assets be relocated to locations which are unaffected by adversary activities?* • *Reconstitute: How quickly can mission-essential functions be restored?* • *Understand: How well does the organization use shared threat information?* • *Transform: How quickly can organizational resources be reassigned to address changing mission needs?* • *Re-Architect: How well does the analysis of the potential effects of adding a new technology to the system consider resilience against adversary attacks?* *The question(s) should be made more specific for a tailored version of the metric, e.g., by identifying specific missions, functions, sub-organizations, assets, or resources.* *Meaning: The discussion can also include (or reference) a description of, or a set of anchoring examples for, the meaning of each identified objective in the context of the organization, program, or system for which the metric is defined. This can include a restatement of the objective, in terms that are more meaningful to stakeholders (e.g., mission owners, program managers, cyber defenders).*
Relationship to Cyber Resiliency Sub-Objective(s) and Activities	Identify the cyber resiliency sub-objectives for which the metric serves as an indicator of achievement. If possible, identify the activities for which the metric supports assessment of how well the activity is performed. Format: "Sub-Objective" or "Sub-Objective: Activities" separated by commas or semi-colons; new paragraph for discussion. *Guidance: The discussion can describe the meaning or interpretation of the relevant sub-objective(s) and activities.*
Relationship to Cyber Resiliency Technique(s) or Approaches	Identify the cyber resiliency technique(s) or implementation approach(es) to which this metric is related. Discuss the relationship of the metric to the technique. Format: "Technique" *or* "Technique: Approach" separated by commas or semi-colons; new paragraph for discussion. *Guidance: Discuss whether and how the metric represents the quality of the application of the technique (e.g., its effectiveness or its assurance) or the extent of the application (e.g., to a subset of relevant resources vs. all relevant resources, at a single layer vs. at all relevant architectural layers). If necessary for clarity and understandability, describe how the technique or approach applies to the system or operational environment for which the metric is evaluated.*
Relationship to Cyber Resiliency Design Principle(s)	Identify the cyber resiliency design principles to which this metric is related. Identify whether the metric represents the quality of the application of the design principle or the extent of the application (e.g., to a subset of relevant resources vs. all relevant resources, at a single layer vs. at all relevant architectural layers). Format: "Design Principle" separated by commas or semi-colons; new paragraph for discussion. *Guidance: Discuss whether and how the metric represents the quality of the application of the design principle or the extent of its application (e.g., to a subset of relevant resources vs. all relevant resources, at a single layer vs. at all relevant architectural layers). If necessary for clarity and understandability, describe how the design principle applies to or what it means in the system or operational environment for which the metric is evaluated.*
Metric Use *The underlined fields must always be populated.*	
Type of system	Identify of describe the type (or types) of system to which the metric applies. *Guidance: Types of system include:* • *All* • *Enterprise information technology (EIT)* • *Federated EIT* • *Large-scale processing environment (LPSE)* • *Cyber-physical system (CPS)*

Template Element	Description and *Guidance*
	• *Federated CPS* • *Platform information technology (PIT)* • *Embedded system* • *Other (specify)* *Metrics which assume a common governance structure and selected general security measures (e.g., firewalls or other boundary protections, identification and authorization, access control, auditing) generally apply to EIT, LPSE, CPS, and PIT. For federated systems – either federated EIT or federated CPS – metrics generally rely on external observations (e.g., externally visible performance characteristics), or on information sharing across organizational boundaries. Metrics for embedded systems generally rely on external observations.*
Intended Use(s) / Type(s) of Decisions Supported	Describe the intended use(s) of the metric – the types of decisions which the metric is intended to support. *Guidance: Examples include:* • *Engineering (e.g., whether and how to apply a CRDP; whether and how to use a cyber resiliency technique, approach, or solution; whether to configure a solution in a specific way). Engineering uses can include setting a threshold or target value, and evaluating technical alternatives to determine whether that target can be met.* • *Administrative / Management (e.g., whether to change operational procedures or practices). Administrative / Management uses can include setting a threshold or target value, and evaluating alternative administrative or management processes, procedures, or practices to determine whether that target can be met.* • *Investment / Programmatic (e.g., whether to acquire a new or different technology; whether to re-design or re-implement a specific component or sub-system; whether to apply resources to training). Investment / Programmatic uses can include setting a threshold or target value, and evaluating investment alternatives to determine whether any of them enable that target to be met.* • *Tactical Operations (e.g., whether to take a specific cyber course of action or CCoA, whether to change system settings or configuration parameters in order to change the system's security or resilience posture)* • *COA Analysis (e.g., whether existing CCoAs or cyber playbooks are meeting operational needs or whether they need to be updated)* *Add further discussion as appropriate to help the reader understand the intended uses and avoid mis-interpreting the metric.*
Domain	Identify the domain which the metric describes [66]. *Guidance: Alternatives are:* • *Physical (e.g., hardware properties, communications speed).* • *Technical / Informational (information about the configuration of, posture or status of, and/or relationships among components, systems, or systems-of-systems).*[40] • *Cognitive (information related to alternative courses of action). Identify whether the metric relates to mission operations, cyber operations (including security administration as well as defensive cyber operations), and/or resource allocation (including staff time allocation as well as allocation of cyber resources, e.g., for performance management).* • *Social / Organizational (information related to organizational structure, communications, and business processes to support Cognitive decisions).*

[40] Note that in [66], this domain is referred to as Informational.

Relationship to Cyber Defense *These fields may or may not be populated, depending on the metric.*	
Relationship to Cyber Security or Cyber Defense MOPs	Identify whether the metric is related to any cyber security (CS) or cyber defense (CS) measures of performance (MOPs) and, if so, whether the relationship is direct (i.e., the same description would be used to identify the CS or CD metric) or indirect. *Guidance: Note that some cyber resiliency metrics are repurposed CS or CD MOPs. If the metric is (or is closely related to) a FISMA metric* [38]*, identify that metric.*
Adversary Behaviors	Describe the adversary behaviors (e.g., TTPs, threat events) against which the metric measures effectiveness. *Guidance: For a generic metric definition, identify the types of adversary activities considered, using the organization's preferred cyber threat framework. For example, identify an attack stage from the ODNI CTF, an ATT&CK category, or an element of the NSA/CSS CTF.* *In a tailored or more specific definition of a metric, this can include identification of specific TTPs, and can involve a reference to a section of a Use Case or can be included as narrative.[41] Note that such specific information may be sensitive.*
Effect(s) on Adversary Activities and Effect-Related Question(s)	Identify the relevant effects on adversary activities for which this metric either provides a direct measure or answers a relevant question. Identify the motivating questions the metric is intended to answer. *Guidance: Adversary activities are as identified in the assumed threat model. Potential effects are Deter, Divert, Deceive, Prevent, Preempt, Degrade, Delay, Detect, Contain, Shorten, Recover, Expunge, Scrutinize, and Reveal.* *Note that in an operational environment, effectiveness against adversary activities can be a performance measure for cyber defenders; thus, this element of the template should be completed in conjunction with the Relationship to Cyber Security or Defense MOPs element.* *Note that potential effects of cyber resiliency techniques on adversary activities in stages in the Cyber Attack Lifecycle have been identified. This mapping can be used as a cross-check between this element of the template and the element on Cyber Resiliency Techniques and Design Principles.* *Note that a mapping between effects on adversary activities and cyber resiliency objectives can be used as a cross-check between this element of the template and the element on Cyber Resiliency Objectives.* *In general, questions take the form "how well is the effect achieved?" (with the corresponding metric being a measure of completeness or effectiveness) or "how quickly can the effect be achieved?" (with the corresponding metric being a measure of timeliness).* *Examples* [1] *include* • *Deter: How strongly are adversaries deterred from attacking the organization?* • *Divert: How well are adversary attacks diverted away from mission-essential resources?* • *Deceive: How long does the adversary operate in the organization's deception environment?* • *Prevent: How many attempts failed because the assumptions underlying the attack technique were invalidated before the attack activity could be executed?* • *Preempt: How many attempts failed because the attack surface changed between adversary reconnaissance and attack delivery?* • *Degrade: How many fewer resources can the adversary affect?* • *Delay: How much longer does it take the adversary to achieve their goals?* • *Detect: How quickly can adversary activity be detected?* • *Contain: How well are adversary activities limited to a single enclave?* • *Shorten: How much shorter is the duration of adversary presence?* • *Recover: How quickly can the consequences of an attack event be rolled back?*

[41] The threat modeling framework proposed in [86] can be used to identify adversary characteristics.

	• *Expunge: How quickly can malware be removed?* • *Scrutinize: How quickly can the organization analyze forensic artifacts?* • *Expose: How effective is the organization's information sharing?* *The question(s) should be made more specific for a tailored version of the metric, e.g., by identifying specific missions, functions, sub-organizations, assets, resources, adversary activities, or consequences; however, such information may be sensitive*.
Relationship to Mission Assurance *These fields may or may not be populated, depending on the metric.*	
Relationship to Mission MOPs	Identify whether the metric is related to any mission measures of performance (MOPs) and, if so, whether the relationship is direct or indirect. *Guidance: If possible (e.g., a metric defined in the context of a specific use case), identify specific mission MOPs.*
Form of Metric *These fields must always be populated.*	
Type of Measurement Scale	Define the type of scale: nominal, ordinal, cardinal, interval, or ratio. *Guidance: Examples of nominal: yes/no, category; ordinal: low/medium/high or 0-10; cardinal: whole numbers; interval: time; ratio: percentage.*
Allowed Values	Define the set of values, or identify the categories, that are valid for the metric (e.g., positive whole numbers only, very high to very low).
Units	Identify or define the units. *Guidance: For nominal or ordinal values, provide a reference to documentation on how to evaluate the metric (e.g., which factors to consider when assigning a value of low vs. medium), or include definitions in the Notes*.
Evaluation *These fields must always be populated.*	
How Obtained	Describe briefly how the metric is evaluated, e.g., measured, observed, derived or computed, judged. Provide amplifying information under Data Collection and Metric Assessment. *Guidance: Select one or more of the following:* • *Measured, using hardware or software tools* • *Observed, by an individual or team* • *Computed or Derived, using an algorithm or a set of heuristic rules, possibly guided by expert judgment or interpretation, using measurements or observations as input* • *Judged, by an individual subject matter expert (SME) or team of SMEs* *In general, time between system-internal events can be measured or observed; time between events involving human activities (e.g., exercises) can be observed; percentages are observed or computed (but if a judgment call is needed, can be judged); counts or numbers can be measured, observed, or judged. Levels of performance or degrees of confidence are judged.*
Evaluation Environment	Describe the expected evaluation environment for the metric. *Guidance: Select one or more of the following:* • *Conceptual environment (e.g., SME analysis of evidence, including observations or documentation)* • *M&S* • *Testing (e.g., in a test environment, on a cyber range)* • *Field Operations* *For a tailored or specific metric, tools, M&S environments, and/or test environments may be identified by name; such specific information may be sensitive.*
Where Measured	*Note: The purpose of providing this description is to enable someone who is considering whether to use the metric to determine whether its evaluation is feasible in their environment.* Identify where the data will be collected (e.g., architectural layer, location in an architectural schematic) *Guidance: Unless otherwise directed, use the following notional layers: physical, hardware*

	/ firmware, networking / communications, system / network component, operating system, cloud / virtualization / middleware infrastructure, service, mission / business process, information store, information stream / feed, personnel / human, organizational process, system / network, system-of-systems.[42]
Data Collection and Metric Evaluation • What • How (process) • Where • When/How Often • Timeframe • By Whom (roles, tools)	*Note: The purpose of providing this description is to enable someone who is considering whether to use the metric to determine whether its evaluation is feasible in their environment.* Describe • What data will be collected • How the data will be collected and translated into an assessed value of the metric (process) • Where the data will be collected (e.g., location(s) in an architectural schematic) • When and how often the data will be collected (e.g., event driven, periodic) • In what timeframe (e.g., hourly, daily, monthly; over the course of a mission execution; over the course of a mission task) • Who or what will collect the data (people, tool). If the process includes a computation, identify the algorithm or specify the formula. Refer to forms or standards if needed. *For a specific or tailored metric, this information may be sensitive.*
Additional Considerations *These fields, if populated, will be free text; alternately or in addition, references to other documents may be provided.*	
Notes	Provide any notes that might be helpful in interpreting or using the metric. *Guidance: Identify which values of the metric are desirable (e.g., higher vs. lower, yes vs. no). Identify what must be done to apply the metric in its target environment. Identify assumptions about the technical environment (e.g., reliance on specific products). Provide references, if available. Indicate whether the metric is related to the conventional Resilience Reference Model (RRM).*
Assumed Context: Threat Model	Describe the characteristics of the adversary (e.g., capabilities, goals) or the non-adversarial threat source assumed by the metric. *Guidance: This can involve a reference to a section of a Use Case, can be included as narrative, or can refer to a framework* [86]. *Characteristics can be drawn from the threat modeling framework provided by Cyber Prep 2.0* [84] *or in* [86]. *For adversarial threats, identification of the adversary's goals in terms of effects on mission, advantages the adversary seeks (e.g., financial gain), and effects in terms of security objectives (e.g., confidentiality, integrity, availability, and accountability) enables those considering the metric to decide whether the cyber resiliency objective(s), sub-objective(s), and activities to which the metric relates are relevant in the context of that adversary. For non-adversarial threats, these can be characterized in terms of the range of effects (see Table D-6 of NIST SP 800-30* [27]*) as well as the impact severity (see Table H-3 of* [27]*).* Identify one or more representative threat scenarios. *Guidance: This can involve a reference to a section of a Use Case or can be included as narrative. See* [86] [84] *for examples of general threat scenarios that can be tailored to be meaningful to a given system or organization.* Identify a set of representative threat events. *Guidance: These events are the building blocks of the representative threat scenarios. For adversarial threats, these can be drawn from the NSA/CSS Technical Cyber Threat Framework* [83]*, ATT&CK, CAPEC, or other taxonomies or lists of threat events. See* [117] *for examples of how general threat events can be tailored to be meaningful in the context of a given system or organization.*
Assumed Context: Operating environment	Describe the operational environment in which the metric definition is meaningful. At a minimum, provide high-level characterizations of

[42] These layers are based on those used in [10] and [5], with the addition of the physical layer to accommodate CPS.

	○ The physical environment and implied or assumed controls (e.g., owner / operator-controlled facility, mobile, hostile) ○ The human environment, including the range of trustworthiness of those (e.g., users, administrators, maintenance personnel, external entities) to whom the system is exposed ○ The cognitive environment for operations (e.g., fully autonomous, human-on-the-loop, human-in-the-loop) *Note: Assumptions about the operational environment influence not only the interpretation of the metric, but also how it can be evaluated. Thus, the discussion of data collection and metric assessment (below) should be consistent with these assumptions.* *Note that some metrics either are repurposed security metrics or might be useful in evaluating how well a given security control is implemented. In the latter case, the 20 types of assumptions and the corresponding alternative values identified in* [118] *may be useful.*

Appendix D SSM-CR

This appendix provides details on the Situated Scoring Methodology for Cyber Resiliency (SSM-CR), which is described at a high level in Section 5.2 above.

D.1 SSM-CR Process

The SSM-CR process is illustrated in Figure 25.

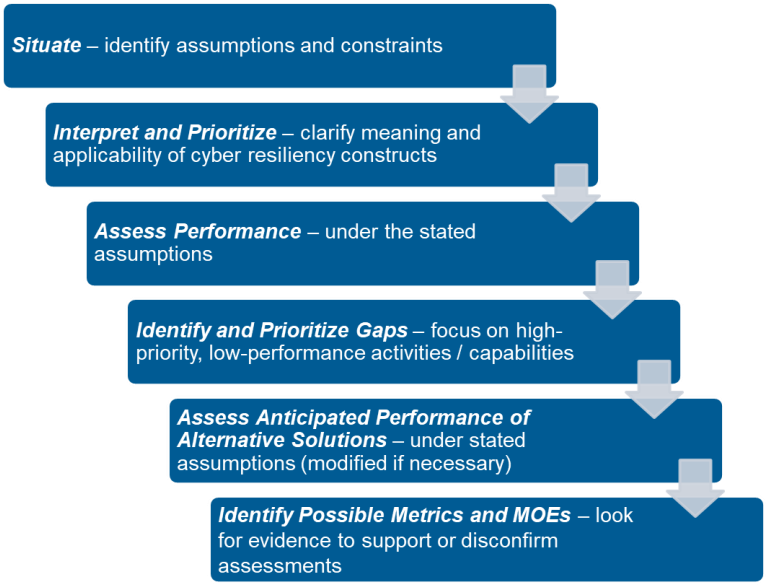

Figure 25. SSM-CR Process

The SSM-CR process consists of the following steps:

- ***Situate*:** A small team of cyber resiliency SMEs interviews stakeholders to identify the system context (including the mission, the operational environment, and programmatic constraints). The team interviews stakeholders and reviews available relevant threat reports to identify the threat context (including adversary goals, intended cyber effects, representative TTPs and attack scenarios). For more information on how to situate the problem of determining cyber resiliency needs, current capabilities, and gaps, see the Use Case report [12].
- ***Interpret and Prioritize*:** The cyber resiliency SMEs describe what cyber resiliency means in this context, working with stakeholders to interpret and prioritize first objectives, then sub-objectives, activities / capabilities in terms meaningful to the mission and system. In the process, some sub-objectives or activities may be deleted or replaced, and additional activities and sub-objectives may be defined. Based on stakeholder inputs, these tailored restatements of cyber resiliency objectives, sub-objectives, and activities are prioritized. Prioritization enables triage: If an objective has zero priority, there is no need to interpret or prioritize its sub-objectives. Similarly, if a sub-objective has zero priority, there is no need to interpret or prioritize the activities which support its achievement.
- ***Assess Performance*:** Depending on the system's maturity and on programmatic constraints, the cyber resiliency SMEs may rely on documentation (e.g., assurance case evidence, documented operational procedures and cyber courses of action), collaborate with systems engineers, or interview mission users and cyber defenders to assess the (actual or projected) ability of the system to perform those activities which have non-zero priority. These assessments are rolled up

into assessments of how well sub-objectives and objectives are achieved, and into an overall cyber resiliency score. The Cyber Resiliency Scorecard Tool (CReST, an Excel workbook) serves as a proof-of-concept tool, using the representative set of sub-objectives and activities in Appendix B.

- ***Identify and Prioritize Gaps*:** Cyber resiliency SMEs, working with systems engineers, identify the activities which are both high-priority and low-performance, as these constitute the most significant capability gaps.
  Based on this gap analysis, relevant cyber resiliency techniques and implementation approaches or techniques are identified (using the tables in Appendix B), and possible solutions (combinations of technologies, architectural decisions, and changes in operational or administrative procedures) can be defined. Definition of possible solutions is not part of SSM-CR, but it is part of the overall SCRAM process which SSM-CR supports. (See Figure 2.)
- ***Assess Anticipated Performance of Alternative Solutions*:** Given a potential solution, cyber resiliency SMEs in collaboration with systems engineers assess the projected ability of the system to perform activities. These assessments are rolled up into assessments of how well cyber resiliency sub-objectives and objectives are achieved. In the course of doing the assessment, the question must be addressed of whether and a solution changes the situation, e.g., by introducing new potential attack scenarios. The results of this assessment of alternative solutions provides a sense of how much overall improvement in cyber resiliency each alternative could provide. In addition, cyber resiliency SMEs can identify the activities for which the changes in the performance assessment were most significant.
- ***Identify Possible Metrics and MOEs*:** Before a solution is acquired or made part of the system, evidence to support or disconfirm the performance assessments is desirable; after a solution is made part of the system, tracking its effectiveness is desirable. Thus, metrics and MOEs for alternative solutions are identified. Cyber resiliency SMEs in collaboration with systems engineers can use the tables in Appendix B or the Cyber Resiliency Metrics Catalog to identify candidate metrics for those activities for which changes in the performance assessment were most significant. As discussed in Appendix A, they can also use changes in mission MOPs or in risk factors as MOEs for the solution.

D.2 Scoring for Cyber Resiliency Objectives, Sub-Objectives, and Activities

To use SSM-CR, stakeholder and SME inputs are used to establish relative priorities of objectives, sub-objectives, and capabilities or activities. Systems engineers then assess the level of performance of activities or the degree to which capabilities exist. Roll-up rules translate the performance assessments of activities or capabilities into performance assessments for sub-objectives, objectives, and overall cyber resiliency. Operational and programmatic constraints can generally be expected to prevent the overall score from reaching 100.

D.2.1 Assess Relative Priorities

Based on stakeholder and SME inputs, each objective is assigned a relevance or priority rating of 0-5, corresponding to the qualitative values of Not Applicable, Very Low, Low, Medium, High, or Very High as described in Table 33. The objectives can and should be restated in terms of mission or business functions and objectives. Similarly, each sub-objective of an applicable objective (i.e., an objective with a non-zero priority rating) is restated and assigned a priority rating. Finally, each activity or capability for an applicable sub-objective is restated and assigned a priority rating. The rationale for assigning the priority ratings is also captured.

Table 33. Relative Priority or Relevance of a Cyber Resiliency Goal, Objective, Sub-Objective, or Capability / Activity

Qualitative Value	Semi-Quantitative Value	Description
Very High	5	Achieving the goal, objective, or sub-objective, providing the capability or performing the activity for the system or for the mission(s) it supports is **crucial** to the organization. The potential consequences of not achieving the goal or objective are **catastrophic**, and might include, for example, permanent or enduring loss of mission capability, destruction of critical assets, or loss of life or life-threatening injuries.
High	4	Achieving the goal, objective, or sub-objective, providing the capability or performing the activity for the system or for the mission(s) it supports is **important** to the organization. The potential consequences of not achieving the goal or objective are **severe**, and might include, for example, severe degradation of mission capability such that one or more critical or essential mission functions cannot be performed, major damage to assets, major financial loss, or serious injuries.
Medium	3	Achieving the goal, objective, or sub-objective, providing the capability or performing the activity for the system or for the mission(s) it supports is **moderately important** to the organization. The potential consequences of not achieving the goal or objective are **serious**, and might include, for example, significant degradation of mission capability such that the effectiveness of one or more critical or essential mission functions is significantly reduced, significant damage to assets, significant financial loss, or significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	2	Achieving the goal, objective, or sub-objective, providing the capability or performing the activity for the system or for the mission(s) it supports is **of low importance** to the organization. The potential consequences of not achieving the goal or objective are **limited**, and might include, for example, degradation of mission capability or minor harm to individuals.
Very Low	1	Achieving the goal, objective, or sub-objective, providing the capability or performing the activity for the system or for the mission(s) it supports is **barely important** to the organization. The potential consequences of not achieving the goal or objective are **minimal**, and might include, for example, minor damage to assets, minor financial loss, or inconvenience to individuals.
N/A	0	The goal, objective, sub-objective, or capability or activity is **not applicable** to the system or to the mission(s) it supports

The representative set of activities or capabilities serves as a starting point, but is oriented toward enterprise information technology and an operational environment which includes ongoing system and network management and a Security Operations Center (SOC) responsible for cyber defense. As the vehicle use case in [12] illustrates, many representative activities can be inapplicable, particularly for a cyber-physical system. The scoring methodology allows different activities to be substituted, or additional activities defined. Similarly, the scoring methodology allows different cyber resiliency sub-objectives to be substituted, or additional sub-objectives defined. However, such substitutions or additions need to be supported by analysis to determine which cyber resiliency techniques and approaches can be used to provide the new activities or capabilities.

D.2.2 Assess Levels of Performance or Quality of Capability

Systems Engineers assess how well each relevant capability is provided (or how well each relevant activity is performed), using the value scale in Table 34. The rationale for assigning a value is also captured.

Table 34. Value Scale for Scoring the Performance of an Activity

Qualitative Value	Semi-Quantitative Value	Description
Very High	5	The capability is provided or the activity is or can be performed **extremely well** in the context of an assumed operational and threat environment. If a set of performance metrics related to the activity is tracked, **all** values **are at or above** target levels.
High	4	The capability is provided or the activity is or can be performed **very well** in the context of an assumed operational and threat environment. If a set of performance metrics related to the objective is tracked, **all** values **fall within acceptable margins** of target levels.
Medium	3	The capability is provided or the activity is or can be performed **adequately** in the context of an assumed operational and threat environment. If a set of performance metrics related to the objective is tracked, **most** values **fall within acceptable margins** of target levels.
Low	2	The capability is provided or the activity is or can be performed **poorly** in the context of an assumed operational and threat environment. If a set of performance metrics related to the goal is tracked, **few** values fall within acceptable margins of target levels; however, performance metrics **may fail to be tracked**, and if they are, target levels **may not be defined**.
Very Low	1	The capability is provided or the activity is or can be performed **very poorly** in the context of an assumed operational and threat environment. If a set of performance metrics related to the goal is tracked, **few if any** values fall within acceptable margins of target levels; however, performance metrics will **usually not** be **tracked**.
N/A	0	The capability or activity is **not applicable** to the system or to the mission(s) it supports.

D.2.3 Roll-Up Rules

The results of SME assessments of capabilities or activities, using the capability / activity priorities as weights, are combined, with the results scaled to lie between 0 and 100, as follows:

- For each relevant **sub-objective**, performance level =
  $100 * (\sum_{activities} Priority(activity) * Performance(activity)) / (\sum_{activities} Priority(activity) * 5)$
  - If all activities have 0 priority, the denominator is set to 1; the result is 0.
  - This formula captures the percentage of the maximum priority-weighted performance achieved by the actual priority-weighted performance.
- For each relevant **objective**, performance level =
  $100 * (\sum_{sub\text{-}objectives} Priority(sub\text{-}objective) * Performance(sub\text{-}objective)) / (\sum_{sub\text{-}objectives} Priority(sub\text{-}objective) * 100)$
  - If all sub-objectives have 0 priority, the denominator is set to 1; the result is 0.

- This formula captures the percentage of the maximum priority-weighted degree of achievement achieved by the actual priority-weighted achievement.

- For **overall cyber resiliency**, performance level =
  $100 * (\sum_{objectives} Priority(objective) * Performance(objective)) / (\sum_{objectives} Priority(objective) * 100)$
  - If all objectives have 0 priority, the denominator is set to 1; the result is 0.
  - This formula captures the percentage of the maximum priority-weighted degree of achievement achieved by the actual priority-weighted achievement.

The Cyber Resiliency Score is on a scale of 0-100. This is to be interpreted as a semi-quantitative value – useful for comparisons, but in no sense absolute or highly granular – since it is computed using semi-quantitative inputs. Thus, the range of 0-20 is Very Low; 21-40 is Low; 41-60 is Moderate; 61-80 is high; and 81-100 is Very High.

D.3 Scoring for Cyber Resiliency Design Principles, Techniques, and Approaches

As discussed in Appendix A, qualitative assessments can also be made for the relevance and quality or extent of application of cyber resiliency design principles and techniques. In addition to the value scales defined for SSM-CR, a set of value scales have been defined to help systems engineers and cyber resiliency SMEs make those assessments for design principles. Because the value scales for structural design principles could easily be adapted for techniques and approaches, only scales for design principles are presented in this Appendix.

D.3.1 Assess Strategic Design Principles

As suggested by the discussion in Sections 2.2 and 3.3, the relevance of a strategic design principle reflects how well it is motivated by or aligned with an organization's or a program's risk management strategy.

Table 35. Relevance of Strategic Cyber Resiliency Design Principles

Qualitative Value	Semi-Quantitative Value	Description
Very High	5	The strategic design principle **directly expresses** one or more **critical** aspects of the organization's risk management strategy, taking into consideration organizational culture, legacy investments and the planned investment strategy, and legal and regulatory constraints.
High	4	The strategic design principle **directly expresses** one or more aspects of the organization's risk management strategy, taking into consideration organizational culture, legacy investments and the planned investment strategy, and legal and regulatory constraints.
Medium	3	The strategic design principle **supports** one or more aspects of the organization's risk management strategy, taking into consideration organizational culture, legacy investments and the planned investment strategy, and legal and regulatory constraints.
Low	2	The strategic design principle **is consistent with** the organization's risk management strategy, taking into consideration organizational culture, legacy investments and the planned investment strategy, and legal and regulatory constraints.

Qualitative Value	Semi-Quantitative Value	Description
Very Low	1	The strategic design principle **is not inconsistent with** the organization's risk management strategy, taking into consideration organizational culture, legacy investments and the planned investment strategy, and legal and regulatory constraints.
N/A	0	The strategic design principle **is not applicable** (e.g., it is inconsistent with one or more aspects of the organization's risk management strategy; it is inconsistent with the organizational culture; it cannot be applied in light of legacy investments and/or the planned investment strategy; or it cannot be applied due to legal or regulatory constraints).

A strategic design principle is applied by analyzing a system, throughout its lifecycle, to determine how well the principle is reflected in the system's architecture, design, implementation, and operational use. Representative analytic resources (e.g., methodologies, processes, tools, frameworks, models) for the strategic cyber resiliency design principles are identified in Table 2 of [3].

Table 36. Extent of Application of Strategic Cyber Resiliency Design Principles

Qualitative Value	Semi-Quantitative Value	Description
Very High	5	The strategic design principle has been applied using **multiple** analytic resources, **throughout** the system lifecycle.
High	4	The strategic design principle has been applied using **multiple** analytic resources, **at key points** the system lifecycle.
Medium	3	The strategic design principle has been applied using **one or more** analytic resources, **at multiple points** in the system lifecycle.
Low	2	The strategic design principle has been applied **analytically** (e.g., in engineering analysis) **at least once** in the system lifecycle.
Very Low	1	The strategic design principle has been applied **notionally** (e.g., in engineering discussions) **at least once** in the system lifecycle.
N/A	0	The strategic design principle **has not been applied**.

D.3.2 Assess Structural Design Principles

Structural design principles are applied to, and embodied in, a system's design. As noted in [3], a cyber resiliency design principle can be applied at a layer (in a notional layered architecture), at identified locations in an architecture or design (e.g., applied to a component or class of component, an enclave, or a subsystem; applied to interfaces between identified subsystems or enclaves). The relevance or potential applicability of a structural cyber resiliency design principle depends on how extensively it can be applied.

Table 37. Relevance of Structural Cyber Resiliency Design Principles

Qualitative Value	Semi-Quantitative Value	Description
Very High	5	**Pervasive**: The structural design principle can be applied at **all (or almost all)** locations or layers.
High	4	**Extensive**: The structural design principle can be applied at **multiple locations or layers**.
Medium	3	**Targeted**: The structural design principle can be applied at **one or a few locations or a single layer**.
Low	2	**Specialized**: The structural design principle can be **interpreted** to apply at **one or a few locations or a single layer**.
Very Low	1	**Minimal**: The structural design principle can be **narrowly interpreted** to apply at **one location or a single layer**.
N/A	0	The structural design principle **is not applicable** to the system.

An assessment of how well a structural cyber resiliency design principle has been applied to a given system, as the value scale in Table 38 describes, is a combination of two factors: how broadly the principle has been applied, and (for each specific application of the principle to a location or at a layer) how well it has been applied. Value scales for these two factors are provided in Tables 39 and 40.

Table 38. Quality of Application of a Structural Cyber Resiliency Design Principle

Qualitative Value	Semi-Quantitative Value	Description
Very High	5	**Excellent**: The structural design principle has been applied **extremely well** at **all** relevant locations or layers.
High	4	**Very Good**: The structural design principle has been applied **well** at **most or many** relevant locations or layers.
Medium	3	**Adequate or Good**: The structural design principle has been applied **fairly well** at **a representative set of** relevant locations or layers.
Low	2	**Inadequate or Poor**: The structural design principle has been **incompletely applied at a few** locations or a single layer, **out of multiple** locations or layers to which it is relevant.
Very Low	1	**Very Poor**: The structural design principle has been **incompletely applied at only one** location, **out of multiple** locations to which it is relevant.
N/A	0	The structural design principle **has not been applied**.

Table 39. Breadth of Application of a Structural Cyber Resiliency Design Principle

Qualitative Value	Semi-Quantitative Value	Description
Very High	5	**Complete**: The structural design principle has been applied at **all** relevant locations or layers.
High	4	**Broad**: The structural design principle has been applied at **most or many** relevant locations or layers.
Medium	3	**Representative**: The structural design principle has been applied at **a representative set of** relevant locations or layers.
Low	2	**Partial**: The structural design principle has been **applied at a few** locations or a single layer, **out of multiple** locations or layers to which it is relevant.
Very Low	1	**Minimal**: The structural design principle has been **applied at only one** location, **out of multiple** locations to which it is relevant.
N/A	0	The structural design principle **has not been applied**.

Table 40. Quality of Single Application of a Structural Cyber Resiliency Design Principle

Qualitative Value	Semi-Quantitative Value	Description
Very High	5	**Excellent**: The structural design principle has been applied **extremely well** at the specified location or layer.
High	4	**Very Good**: The structural design principle has been applied **well** at the specified location or layer.
Medium	3	**Adequate or Good**: The structural design principle has been applied **fairly well** at the specified location or layer.
Low	2	**Inadequate or Poor**: The structural design principle has been **poorly or incompletely applied** at the specified location or layer.
Very Low	1	**Very Poor**: The structural design principle has been **very poorly or very incompletely applied** at the specified location or layer.
N/A	0	The structural design principle **has not been applied**.

Appendix E Glossary

Term	Definition
Advanced Persistent Threat (APT)	An adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat: (i) pursues its objectives repeatedly over an extended period of time; (ii) adapts to defenders' efforts to resist it; and (iii) is determined to maintain the level of interaction needed to execute its objectives. [119]
Asset	An item of value to stakeholders. An asset may be tangible (e.g., a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (e.g., humans, data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, or reputation). The value of an asset is determined by stakeholders in consideration of loss concerns across the entire system life cycle. Such concerns include but are not limited to business or mission concerns. [2]
Attack surface	The set of resources and vulnerabilities that are exposed to potential attack.
Component	A part of a system that can be replaced or managed separately from other parts of the system. Examples of components include hardware devices, embedded devices (e.g., sensors, controllers, medical devices such as pacemakers, vehicle automation such as collision avoidance), desktop or laptop computers, servers, routers, firewalls, virtual machine monitors (VMMs) or hypervisors, operating systems (OSs), applications, and databases. When "system" is construed as a socio-technical system, examples also include people and separately managed processes.
Constituent system	A system, viewed as an element of a system-of-systems.
Cyber asset	A cyber resource which is an asset.
Cyber course of action (CCoA)	A set of activities or tactics, techniques, and procedures (TTPs) employed by automation, cyber defenders (e.g., staff in a Security Operations Center (SOC) or a Cyber Security Operations Center) and, as needed, other cyber staff (e.g., staff in a Cyber Operations Center, system administrators, network operators) and mission staff or end users in response to threat events. [4] CCoAs can be defined solely for adversarial threats, in which case the documentation of CCoAs takes the form of a "cyber playbook."
Cyber effect	A change that is caused by a cyber event (such as degradation, interruption, modification, fabrication, unauthorized use, interception) on a cyber resource. [120] [29]

Term	Definition
Cyber-physical system (CPS)	A smart system that includes engineered interacting networks of physical and computational components. [121] "Cyber-physical systems integrate sensing, computation, control and networking into physical objects and infrastructure, connecting them to the Internet and to each other." [122] Note: As discussed in [121], CPSs range from devices to systems to systems-of-systems. Unless otherwise specified (e.g., CPS device, stand-off CPS), the term CPS is interpreted to refer to a system-of-systems which includes as constituent systems both CPS devices and IT [123] [124].
Cyber-physical device or CPS device	A device that has an element of computation and interacts with the physical world through sensing and actuation. [125]
Cyber playbook	An action plan that documents an actionable set of steps an organization can follow to successfully recover from a cyber event. [126] More broadly, a cyber playbook documents actionable steps to respond to indicators, warnings, suspicious events, and evidence of adversity.
Cyber resource	An information resource which creates, stores, processes, manages, transmits, or disposes of information in electronic form and which can be accessed via a network or using networking methods.
Cybersecurity	The activity or process, ability or capability, or state whereby information and communications systems and the information contained therein are protected from and/or defended against damage, unauthorized use or modification, or exploitation. [127] The ability to protect or defend the use of cyberspace from cyber attacks. [128] [129]
Cyberspace	The interdependent network of information technology infrastructure, including the Internet, telecommunications networks, computers, information and communications systems, and embedded processors and controllers. [130]
Data asset	Data and information required to execute business or mission functions, deliver services, and for system management and operation; sensitive data and information (e.g., classified information, controlled unclassified information, proprietary data, trade secrets, privacy information, critical program information, and intellectual property); and all forms of documentation associated with the system. [2]
Dynamic	Occurring (or capable of occurring) without interrupting or suspending operations.

Term	Definition
Embedded device or embedded system	Computer system designed to perform one or a few dedicated functions often with real-time computing constraints. Note 1 to entry: It is embedded as part of a complete device often including hardware and mechanical parts. By contrast, a general-purpose computer, such as a personal computer (PC), is designed to be flexible and to meet a wide range of end-user needs. Embedded systems control many devices in common use today. Note 2 to entry: In general, “embedded system" is not a strictly definable term, as most systems have some element of extensibility or programmability, e.g. hand-held computers share some elements with embedded systems such as the operating systems and microprocessors which power them, but they allow different applications to be loaded and peripherals to be connected. Moreover, even systems which don't expose programmability as a primary feature generally need to support software updates. On a continuum from “general purpose" to “embedded," large application systems will have subcomponents at most points even if the system as a whole is “designed to perform one or a few dedicated functions," and is thus appropriate to call “embedded." [131]
Enterprise information technology (EIT)	The application of computers and telecommunications equipment to store, retrieve, transmit, and manipulate data, in the context of a business or other enterprise. [1] Note: EIT typically includes an enterprise-internal networking infrastructure; end-user clients, with local applications for Web browsing, email, word processing, and spreadsheet use; servers for enterprise applications and data; and an interface between the enterprise network and the Internet, which includes proxy servers on a demilitarized zone (DMZ).
Federated CPS	A CPS system-of-systems consisting of multiple constituent CPSs owned and/or operated by different organizations or mission / business process owners. A federated CPS usually includes some general-purpose system elements typical of EIT.
Federated EIT	A federated architecture within an enterprise or a federation across multiple enterprises. In federated EIT, business or mission information is exchanged across semi-autonomous or autonomous organizations, lines of business, and information systems.
Functional dependency map	A graph or other visual representation of functional dependencies among components.
Information asset	See *data asset*.
Information security	The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability. [129]
Key Performance Parameter (KPP)	A performance attribute of a system considered critical or essential to the development of an effective military capability. KPPs are expressed in term of parameters which reflect Measures of Performance (MOPs) using a threshold/objective format. [132]
Large-Scale Processing Environment (LPSE)	A system which enables large numbers of events to be handled (e.g., transactions to be processed) with high confidence in service delivery. The scale of such systems makes them highly sensitive to disruptions in or degradation of service. [1] Note: An enterprise architecture may include one or more instances of LSPEs, which typically involve high-volume transaction processing and/or big data analytics [133].

Term	Definition
Measure of Effectiveness (MOE)	An indicator used to measure a current system state, with change indicated by comparing multiple observations over time. [14]
	A measure designed to correspond to accomplishment of mission objectives and achievement of desired results. MOEs quantify the results to be obtained by a system and may be expressed as probabilities that the system will perform as required. MOEs may be further decomposed into Measures of Performance and Measures of Suitability. [132]
Measure of Performance (MOP)	A system-particular performance parameter such as speed, payload, range, time-on-station, frequency, or other distinctly quantifiable performance feature. Several MOPs may be related to the achievement of a particular Measure of Effectiveness (MOE). [132]
Mission / business function	An activity, task, process, or set of related activities, tasks, or processes intended to achieve a mission or business objective.
Mission-critical	Critical to the successful execution of a mission, mission task, or mission function.
Mission damage	The decrease in the ability to complete the current mission and to accomplish future missions. Mission damage may be assessed in terms of mission measures of effectiveness (MOEs), system measures of performance (MOPs), or Key Performance Parameters (KPPs) of system elements.
Mission dependency map	A graph or other visual representation of dependencies between mission tasks and of mission tasks on cyber, physical, and personnel resources.
Mission-supporting	Supportive of a mission task or mission function.
Mission thread	A sequence of end-to-end activities and events that takes place to accomplish the execution of an SoS capability. [134]
Platform	(1) A platform is comprised of one or more devices assembled and working together to deliver a specific computing function, but does not include any other software other than the firmware as part of the devices in the platform. Examples of platforms include a notebook, a desktop, a server, a network switch, a blade, etc. [61]
	(2) A vehicle, structure or person that performs a mission in support of US National Security policy; and aboard or in which a DoD national security system may be installed to support assigned missions. Generally, the term “platform” includes, but is not limited to, Aircraft, Ship, Submarine, Shore Facility (such as NOC, JIC, Command Center, Hospital, Base Power Plants), Ground Vehicle (such as HMMWVs, Tanks, Strykers), Remotely Operated Vehicle (such as UAV, USV, UUV), and a Sailor or Marine in the field. [135]
Platform IT	IT, both hardware and software, that is physically part of, dedicated to, or essential in real time to the mission performance of special-purpose systems. [136] [137]
	Note: Platform IT is part of a platform in the sense of [135].
Resilience reference model	A model used in survivability or resilience engineering in which (i) performance or functionality is represented over time, (ii) adverse conditions, incidents, or disruptions can be represented as discrete events in time and are detectable, and (iii) full or partial recovery from those disruptions can be achieved.
Resource	A component of, or a service or capability provided by, a system, which can be used by multiple mission / business functions. General examples include staff (e.g., system operators, administrators), communications bandwidth, processing, and storage. Other examples are more system- or mission/business process-specific, and can include information resources (e.g., data of a specified quality) as well as computing or networking services subject to service-level agreements (SLAs).

Term	Definition
Security	Freedom from those conditions that can cause loss of assets with unacceptable consequences. [2] A condition that results from the establishment and maintenance of protective measures that enable an enterprise to perform its mission or critical functions despite risks posed by threats to its use of information systems. Protective measures may involve a combination of deterrence, avoidance, prevention, detection, recovery, and correction that should form part of the enterprise's risk management approach. [128] [129] Often construed as *information security* or *cybersecurity* (see above), due to use in statute. For example, one definition of security in https://csrc.nist.gov/Glossary/?term=1189#AlphaIndexDiv is: Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide— (A) integrity, which means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity; (B) confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and (C) availability, which means ensuring timely and reliable access to and use of information. [138], (44 U.S.C., Sec. 3542)
Security-critical	Critical to achieving the security objectives of confidentiality, integrity, availability, and accountability, and/or to successfully executing the security functions of identify, protect, detect, respond, and recover.
Stand-off	Capable of operating (at least transiently) without a network connection. Note: A system operating in stand-off mode differs from a stand-alone system in that it is intended to have network connectivity, but is capable of operating without network connectivity under some circumstances. Platform IT is typically stand-off. A stand-off system can, but does not have to, be autonomous or semi-autonomous. For example, a wearable insulin pump is a semi-autonomous system which operates in stand-off mode, but can connect to a healthcare provider's network for data sharing and analysis as well as software updates.
System-of-Systems (SoS)	A system whose elements are themselves systems [2]; these are referred to as *constituent systems*. "*A system of systems (SoS) brings together a set of systems for a task that none of the systems can accomplish on its own. Each constituent system keeps its own management, goals, and resources while coordinating within the SoS and adapting to meet SoS goals.*" [139], Annex G
Tactics, Techniques, and Procedures (TTPs)	The use of capabilities and resources in relation to each other (tactics); non-prescriptive ways or methods used to perform missions, functions, or tasks (techniques); and standard, detailed steps that prescribe how to perform specific tasks (procedures) ([140], adapted).

Appendix F Abbreviations and Acronyms

AD	Active Directory
APT	Advanced Persistent Threat
ATT&CK™	Adversarial Tactics, Techniques & Common Knowledge
BIA	Business Impact Analysis
CAN	Controller Access Network
CDM	Continuous Diagnostics and Monitoring
CIO	Chief Information Officer
CIS	Center for Internet Security
CISS	Cyber Incident Severity Schema
CCoA	Cyber Course of Action
CERT	Computer Emergency Response Team
CIS	Center for Internet Security
CJA	Crown Jewels Analysis
CNSS	Committee on National Security Systems
CNSSI	CNSS Instruction
COA	Course of Action
CONOPS	Concept of Operations
COOP	Continuity of Operations
COTS	Commercial Off-The-Shelf
CPS	Cyber-Physical System
CRDP	Cyber Resiliency Design Principles
CREF	Cyber Resiliency Engineering Framework
CSF	[NIST] Cybersecurity Framework
CSG	Cyber Security Game
CSIAC	Cyber Security and Information Systems Information Analysis Center
CTF	Cyber Threat Framework
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CWE	Common Weakness Enumeration
CWSS	Common Weakness Scoring System
DNS	Domain Name Service
DoD	Department of Defense
DON	Department of the Navy

EA	Enterprise Architecture
EPRI	Electric Power Research Institute
EIT	Enterprise IT
FISMA	Federal Information Security Management Act
GQM	Goal-Question-Metric
IATAC	Information Assurance Technology Assurance Center
ICS	Industrial Control System
IDS	Intrusion Detection System
IEEE	Institute of Electrical and Electronics Engineers
ISO	International Standards Organization
IT	Information Technology
KES	Keyless Entry System
KPP	Key Performance Parameter
KSA	Key System Attribute
LSPE	Large-Scale Processing Environment
M&S	Modeling and Simulation
MBSE	Model-Based Systems Engineering
MECR	Measuring the Effectiveness of Cyber Resiliency
MIA	Mission Impact Analysis
MIP	MITRE Innovation Program
MOE	Measure of Effectiveness
MOP	Measure of Performance
MTR	MITRE Technical Report
NCCIC	National Cybersecurity and Communications Integration Center
NCISS	NCCIC Cyber Incident Scoring System
NICCS	National Initiative for Cybersecurity Careers and Studies
NIST	National Institute of Standards and Technology
NSA/CSS	National Security Agency / Central Security Service
ODNI	Office of the Director of National Intelligence
OEM	Original Equipment Manufacturer
PIT	Platform IT
POET	Political, Operational, Economic, and Technical
RRM	Resilience Reference Model
SCRAM	Structured Cyber Resiliency Analysis Methodology
SLA	Service-Level Agreement
SME	Subject Matter Expert

SP	[NIST] Special Publication
SOC	Security Operations Center
SoS	System-of-Systems
SRP	Shared Research Program
SSM-CR	Situated Scoring Methodology for Cyber Resiliency
TTP	Tactic, Technique, or Procedure
TTPs	Tactics, Techniques, and Procedures
VM	Virtual Machine
VODEA	Vocabulary for Describing Effects on Adversary Activities
WS	Weapon System