MTR180450

MITRE TECHNICAL REPORT

Cyber Resiliency Metrics Catalog

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

The views, opinions and/or findings contained in this report are those of The MITRE Corporation and should not be construed as an official government position, policy, or decision, unless designated by other documentation.

NOTICE

This technical data was produced for the U. S. Government under Contract No. FA8702-18-C-0001, and is subject to the Rights in Technical Data-Noncommercial Items Clause DFARS 252.227-7013 (JUN 2013)

Bedford, MA

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

September 2018

Abstract

Cyber resiliency – *the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on cyber resources* – is increasingly an explicit concern at varying scopes or scales, ranging from components to critical infrastructure sectors, regions, and nations. Systems engineers and architects need ways to evaluate the relative effectiveness of architectural alternatives, as well as new technologies, products, or processes, for improving cyber resiliency and mission assurance. Nearly 500 representative cyber resiliency metrics have been captured in a searchable catalog, which is described in this report.

Table of Contents

List of Figures

List of Tables

This page intentionally left blank.

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]. 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].

This report presents a catalog of cyber resiliency metrics that can be used by systems engineers and cyber defenders to describe how well their efforts enable the cyber resiliency objectives to be achieved. The catalog presented in this report supersedes the earlier cyber resiliency metrics catalog published by The MITRE Corporation in 2012 [7]. The catalog also is captured in an Excel workbook. Section 2 briefly describes the fields in the catalog. Each entry in the metrics catalog – each generic or tailorable metric – is intended to serve as the starting point for a more complete definition (e.g., using the template in [8]).

The catalog is provided in Appendix A. It was produced by the Measuring the Effectiveness of Cyber Resiliency (MECR) research project team funded by the MITRE Innovation Program.

This report is not intended to provide background. For information about cyber resiliency, including the Cyber Resiliency Engineering Framework (CREF), see [1]. For discussion of how cyber resiliency metrics can be characterized and derived, and how the cyber resiliency metrics catalog can be used, see the report on Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring [8].

2 Fields in the Cyber Resiliency Metrics Catalog

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, the domain to which it relates, and how it can be evaluated. 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 system or set of circumstances. A tailored metric can be more fully specified by using the Cyber Resiliency Metric Template [8]; 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. This section briefly describes the fields (identified in ***bold italics***) of fields in the catalog.

2.1 Metric Identification

2.1.1 Metric Identifier

Each metric in the catalog has a ***metric identifier***. Most of the metrics derive from Appendix B of [8], in which sub-objectives are defined for each cyber resiliency objective, activities which support achieving sub-objectives are identified, and representative metrics for those activities are then identified. These have identifiers of the form OO-S#-A#-#. OO refers to the cyber resiliency 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, A# indicates the activity. (Note that a given metric can relate to multiple objectives, sub-objectives, or activities; the identifier comes from the first of these for which the metric was identified.) A final number is assigned to identify the metric; for example, RE-S1-A3-1 is the first metric defined for the third activity supporting the first sub-objective for the Reconstitute objective.

A few metrics in the catalog were defined from cyber resiliency techniques and approaches. These have identifiers of the form TE-AP-#, where TE is a two-letter abbreviation of the technique and AP is a two-letter abbreviation of the approach. Similarly, a few metrics in the catalog were defined from the cyber resiliency design principles [3]; these have identifiers of the form ST-#-#, where ST indicates the metric is motivated by a structural design principle and the first number is the number of that design principle.

Some metrics have been carried forward from the 2012 cyber resiliency metrics catalog [7]; the identifiers for these are of the form MT-#. Gaps in the numbering of metrics with identifiers of the form MT-# are primarily due to the fact that the 2012 catalog was populated by multiple individuals. However, some of the metrics in the 2012 catalog have not been carried forward, as experience showed that more detailed specification or practical evaluation was problematic.

2.1.2 Metric Descriptor

Each metric in the catalog has a ***metric descriptor***. This is a short phrase describing what is being measured. The description suggests the form of the metric, e.g., number, percentage, time, degree. Note that any such description needs to be amplified. The Cyber Resiliency Metrics Template provides fields for the form of the metric, as well as how and where the metric is evaluated. That description of "how" can include definitions of terms in the metric descriptor as well as explanations of how terms apply to a given system or environment.

2.2 Relationship to Cyber Resiliency

2.2.1 Cyber Resiliency Objective

For each metric in the catalog, at least one ***cyber resiliency objective*** is identified. The metric serves as an indicator of how well that objective is achieved. Note that many metrics can serve as indicators of multiple cyber resiliency objectives.

2.2.2 Cyber Resiliency Sub-Objective and Activity

For most metrics in the catalog, at least one ***sub-objective*** of the identified cyber resiliency objective(s) is identified. The metric serves as an indicator of how well that sub-objective is achieved. For most metrics in the catalog, one or more ***activities*** that support achieving the identified sub-objective are also identified. When this is the case, the metric supports assessment of how well the activity is performed. The format of the field is "Sub-Objective" or "Sub-Objective: Activity." Multiple values are separated by commas or semi-colons.

2.2.3 Cyber Resiliency Technique or Approach

For each metric in the catalog, at least one cyber resiliency ***technique*** is identified. For most metrics in the catalog, at least one implementation ***approach*** is identified for each identified technique. The metric serves as an indicator of how well (how effectively or with how much assurance) the technique or approach is applied, 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). The format of the field is "Technique" or "Technique: Approach." Multiple values are separated by commas or semi-colons.

2.2.4 Cyber Resiliency Design Principle

For each metric in the catalog, at least one structural cyber resiliency ***design principle*** is identified. (See [3] or Appendix F of [1] for more information about cyber resiliency design principles.) The metric serves as an indicator of how well (how effectively or with how much assurance) the design principle is applied, or the extent of its application (e.g., to a subsystem vs. the system as a whole, at a single layer vs. at all relevant architectural layers). As noted in [3], more specific restatements of structural cyber resiliency design principles can aid in their application to a given system or environment. If a metric relates to a restatement, that is also captured. The format of the field is "Design Principle" or "Design Principle: Restatement." Multiple values are separated by commas or semi-colons.

2.3 Metric Use

2.3.1 Type of System

For each metric in the catalog, the ***type or types of systems*** for which it can meaningfully be defined are identified. The type of system implicitly indicates a generic set of architectural elements, as well as the aspect of governance which influences or determines what information can be collected. Metrics in the catalog relate to one or more of the following types:

- Enterprise information technology (EIT). EIT typically includes a network; servers for mission or business applications; servers and user endpoint devices for communications applications (e.g., email, instant messaging), Internet-facing applications (e.g., Web browser), and data manipulation applications (e.g., word processing, spreadsheets, database management systems); enterprise services such as identity and access management (IdAM) and domain name service (DNS); and firewalls between the enterprise and the Internet. Data can typically be gathered for each of these architectural elements, and can be shared with enterprise-level security monitoring and performance management services. However, for some enterprises, EIT sufficiently large and complex that it may more closely resemble federated EIT.

- Federated EIT. Federated EIT consists of enclaves of EIT, with defined communications and control paths between them. The different enclaves can have different technical architectures (e.g., conforming to different suites of technical standards).
- Large-scale processing environment (LPSE). An LSPE is 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 [9].
- Cyber-physical system (CPS). A CPS is a smart system that includes engineered interacting networks of physical and computational components [123]. As discussed in [10], 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 information technology (IT) [11] [12].
- Federated CPS. A federated CPS is a 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.
- Platform information technology (PIT). PIT is 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 [13] [14]. Platform IT is part of a platform in the sense of [15]; that is, a platform is a vehicle (terrestrial, airborne, space, or maritime). A PIT architecture typically combines elements of CPS and EIT architectures. However, a distinguishing characteristic of a platform is that it is mobile, and may need to operate with limited or no network connectivity during the execution of specific mission tasks.

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. Some metrics may be inapplicable to PIT (or applicable only under specific operational conditions, e.g., in garrison vs. in the field), due to network or staff limitations.

2.3.2 Intended Uses

For each metric in the catalog, its possible **intended use** or uses – i.e., the types of decisions it is intended to support – are identified. Metrics in the catalog are intended for the following uses:

- Engineering (e.g., whether and how to apply a cyber resiliency design principle; 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). Tactical Operations uses typically consider the values of cyber resiliency metrics in conjunction with information about mission status and system performance.
- COA Analysis (e.g., whether existing CCoAs or cyber playbooks are meeting operational needs or whether they need to be updated). COA Analysis can use trends in metrics related to Tactical Operations.

Many of the metrics in the catalog can be used to support multiple types of decisions. A metric for which a specific evaluation process is specified may only be suitable for a single type of decision. For example, the average time to perform a damage assessment (AM-DA-1) can be measured in a laboratory, via modeling and simulation (M&S), or at a cyber range, or it can be computed or derived from operational experience. If the evaluation is in a laboratory or M&S environment, the results relate to the technical capabilities provided by the system and support Engineering decisions. If the evaluation is in a cyber range or an operational environment, the results relate to how well the technical capabilities can be used in practice. That information supports COA Analysis (new or modified COAs may be needed to provide timely and useful damage assessments) and may also support Tactical Operations (the choice of a CCoA may depend on how quickly a damage assessment can be performed). Thus, a fully specified metric (i.e., the populated Cyber Resiliency Metric Template) may identify only one or two of the multiple types of decisions identified in the catalog entry.

2.3.3 Domain

For each metric in the catalog, the ***domain*** or set of domains which the metric describes is identified. For more information, see [16] [17] [18] [19]. Metrics in the catalog can relate to one or more of the following domains:

- Physical (e.g., hardware properties, communications speed).

- Information / Technical (information about the configuration of, posture or status of, and/or relationships among components, systems, or systems-of-systems).[1]
- Cognitive (information related to alternative courses of action). The catalog entry can 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).

Most of the entries in the catalog relate to the Information / Technical or Cognitive domains, although some relate to the Social / Organizational domain.

2.4 How Metric Values Are Obtained

For each metric in the catalog, the ***how obtained*** field identifies (in general terms) how the metric can be evaluated. (The Cyber Resiliency Metric Template enables details about how data is collected, if applicable where in the system data is collected, what formulas or algorithms are used, etc. to be captured.) Metrics in the catalog can be evaluated using one or more of the following methods:

- 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.

[1] Note that in [17], this domain is referred to as Informational.

3 Concept of Use for the Catalog

The cyber resiliency metrics catalog can be used in a variety of ways. This section provides a few notional examples.

3.1 Evaluate a Proposed Solution

Frequently, a change to an existing system is proposed, based on promulgation of a new technology or product, awareness of a new attack pattern, or negative experiences with system operation. In order to evaluate the potential benefits (or increased risks) of that proposed change, metrics can be selected from the catalog based on the system type and the domain in which the change is made (e.g., Information / Technical for introduction of a new product, Cognitive for a change in CCoAs). If the proposed change is claimed to improve how well a given cyber resiliency objective is achieved or how well a given cyber resiliency technique or design principle is applied, these fields can also be used in metric selection.

3.2 Metrics for a Cyber Resiliency Use Case

A cyber resiliency use case is a notional worked example of how cyber resiliency concepts and constructs can be interpreted and applied to a specific situation, cyber resiliency solutions can be defined for that situation, and the relative effectiveness of alternative solutions compare in that situation. Use cases illustrate how cyber resiliency can be applied in a variety of ways, depending on the situation (i.e., the mission, system architecture, threat model, risk management strategy, and programmatic constraints). The use case process is illustrated in Figure 1 below.

For the MECR project, a use case is also intended to illuminate how cyber resiliency metrics, measures of effectiveness (MOEs) or measures of performance (MOPs), and scoring can be used to inform decisions. More detail on the use case methodology can be found in [20]. As illustrated in Figure 1, cyber resiliency (CR) metrics are identified in a use case to evaluate how well a potential solution fills a functional gap, improves mission performance, or reduces risk associated with a threat. Metrics in the catalog relate to functional gaps.

The developer of a use case looks at which activities cannot be performed to a satisfactory degree, and searches the catalog for metrics which relate to those activities. That set is further refined based on the type of system and the type of decision posited by the use case. The developer of the use case complements these with metrics and MOEs related to mission performance and/or risk. Depending on the scope of the use case, some metrics may be fully or notionally specified, using the Cyber Resiliency Metric Template.

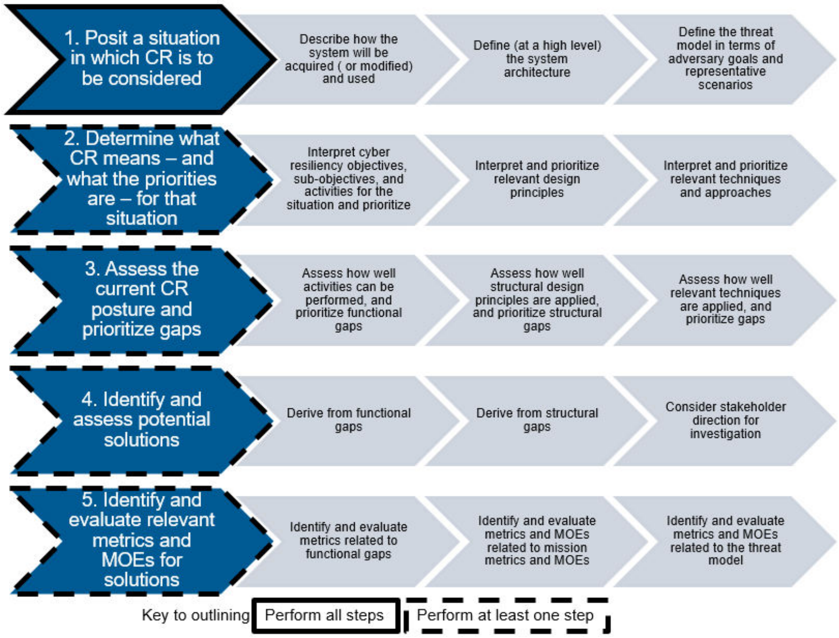
1. Posit a situation in which CR is to be considered
Describe how the system will be acquired (or modified) and used
Define (at a high level) the system architecture
Define the threat model in terms of adversary goals and representative scenarios
2. Determine what CR means – and what the priorities are – for that situation
Interpret cyber resiliency objectives, sub-objectives, and activities for the situation and prioritize
Interpret and prioritize relevant design principles
Interpret and prioritize relevant techniques and approaches
3. Assess the current CR posture and prioritize gaps
Assess how well activities can be performed, and prioritize functional gaps
Assess how well structural design principles are applied, and prioritize structural gaps
Assess how well relevant techniques are applied, and prioritize gaps
4. Identify and assess potential solutions
Derive from functional gaps
Derive from structural gaps
Consider stakeholder direction for investigation
5. Identify and evaluate relevant metrics and MOEs for solutions
Identify and evaluate metrics related to functional gaps
Identify and evaluate metrics and MOEs related to mission metrics and MOEs
Identify and evaluate metrics and MOEs related to the threat model
Key to outlining
Perform all steps
Perform at least one step

Figure 1. Use Case Process

3.3 Organizational Metrics Program

An organization can create a cyber resiliency metrics program, as part of its larger cyber risk management, cyber resiliency, or cybersecurity metrics program. To identify metrics the organization might track, program staff would search the catalog for metrics in the Social / Organizational domain. They would select a few of these for further definition, evaluation, and tracking. To gain more insight into the effectiveness of the organization's cyber risk management, cyber resiliency, or cybersecurity program, they could also identify the types of systems the organization operates, and search for metrics for each type of system. (In general, different sub-organizations are responsible for different types of systems. For example, a critical infrastructure provider might have one sub-organization responsible for CPS and another for EIT.) This would produce an initial set, from which down-selection would be needed. To down-select, program staff would execute the first two steps of the Situated Scoring Methodology for Cyber Resiliency (SSM-CR) [8], focusing on interpreting the cyber resiliency objectives, sub-objectives, and activities in terms From those, they could focus on metrics which provide evidence of how well the highest-priority activities can be performed. A variety of metrics – supporting different decisions, in different domains, and evaluated in different ways – can be selected for specification using the Cyber Resiliency Metric Template, evaluated, and tracked.

Because it is in the form of a table or Excel workbook, the catalog is easily extensible. Therefore, if an organization defines new metrics, or finds ways to reuse existing performance, system resilience, or security metrics to describe cyber resiliency, these can be added.

4 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, 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.

[8] D. J. Bodeau, R. D. Graubart, R. M. McQuaid and J. R. Woodill, "Cyber Resiliency Metrics, Measures of Effectiveness, and Scoring: Enabling Systems Engineers and Program Managers to Select the Most Useful Assessment Methods (MTR180314, PR 18-2579)," The MITRE Corporation, Bedford, MA, 2018.

[9] 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.

[10] 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.

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

[12] 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.

[13] 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.

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

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] D. Bodeau, R. Graubart, R. McQuaid and J. Woodill, "Cyber Resiliency Scoring and Metrics in Practice: Use Case Methodology and Examples (MTR180449)," The MITRE Corporation, Bedford, MA, 2018.

Appendix A Catalog

Table 1. Cyber Resiliency Metrics Catalog

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
AM-DA-1	Elapsed time for [mission / system / asset] damage assessment	Continue	Minimize degradation of service delivery: Perform mission damage assessment; Minimize interruptions in service delivery: Perform mission damage assessment	Analytic Monitoring: Monitoring and Damage Assessment; Dynamic Representation: Mission Dependency and Status Visualization; Substantiated Integrity: Integrity Checks, Behavior Validation	Leverage health and status data	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations, COA Analysis	Information / Technical, Cognitive (Cyber Operations), Social / Organizational	Measured or Observed, Computed or Derived
DP-FR-1	Percentage of services which can be relocated virtually (e.g., to another virtual machine)	Prevent / Avoid, Continue, Constrain	Limit exposure to threat events: Dynamically relocate processing randomly or in response to a triggering event; Minimize degradation of service delivery: Relocate resources to minimize service degradation; Move resources to limit future or further damage: Relocate targeted resources	Adaptive Response: Adaptive Management; Dynamic Positioning: Functional Relocation of Cyber Resources	Manage resources (risk-)adaptively, Leverage health and status data	EIT, LSPE	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Observed
DP-FR-2	Percentage of resources which can be virtually relocated automatically	Prevent / Avoid, Continue	Limit exposure to threat events: Dynamically relocate processing randomly or in response to a triggering event; Minimize degradation of service delivery: Relocate resources to minimize service degradation	Adaptive Response: Adaptive Management; Dynamic Positioning: Functional Relocation of Cyber Resources	Manage resources (risk-)adaptively, Leverage health and status data	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
DP-FR-3	Average time to complete the virtual relocation process (latency or lag)	Prevent / Avoid, Continue, Constrain	Limit exposure to threat events: Dynamically relocate processing randomly or in response to a triggering event; Minimize degradation of service delivery: Relocate resources to minimize service degradation; Move resources to limit future or further damage: Relocate targeted resources	Adaptive Response: Adaptive Management; Dynamic Positioning: Functional Relocation of Cyber Resources	Manage resources (risk-)adaptively, Leverage health and status data	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Observed, Computed or Derived
DP-AM-1	Percentage of resources which can be relocated physically (e.g., to a backup facility)	Prevent / Avoid, Continue, Constrain	Limit exposure to threat events: Dynamically relocate processing randomly or in response to a triggering event; Minimize degradation of service delivery: Relocate resources to minimize service degradation; Move resources to limit future or further damage: Relocate targeted resources	Adaptive Response: Adaptive Management; Dynamic Positioning: Asset Mobility	Manage resources (risk-)adaptively, Leverage health and status data	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Observed, Computed or Derived
DP-AM-2	Percentage of resources which can be physically relocated automatically	Prevent / Avoid, Continue	Limit exposure to threat events: Dynamically relocate processing randomly or in response to a triggering event; Minimize degradation of service delivery: Relocate resources to minimize service degradation	Adaptive Response: Adaptive Management; Dynamic Positioning: Asset Mobility	Manage resources (risk-)adaptively, Leverage health and status data	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
DP-AM-3	Average time to complete the physical relocation process (latency or lag)	Prevent / Avoid, Continue, Constrain	Limit exposure to threat events: Dynamically relocate processing randomly or in response to a triggering event; Minimize degradation of service delivery: Relocate resources to minimize service degradation; Move resources to limit future or further damage: Relocate targeted resources	Adaptive Response: Adaptive Management; Dynamic Positioning: Asset Mobility	Manage resources (risk-)adaptively, Leverage health and status data	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Observed, Computed or Derived
PV-DP-1	Percentage of cyber resources for which privileges can be modified dynamically	Prevent / Avoid	Limit exposure to threat events: Modify privilege restrictions unpredictably	Privilege Restriction: Dynamic Privileges; Unpredictability: Temporal Unpredictability, Contextual Unpredictability	Manage resources (risk-)adaptively	EIT, Federated EIT, LSPE	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed (tool settings)
PV-DP-2	Percentage of users for whom privileges can be modified dynamically	Prevent / Avoid	Limit exposure to threat events: Modify privilege restrictions unpredictably	Privilege Restriction: Dynamic Privileges; Unpredictability: Temporal Unpredictability, Contextual Unpredictability	Manage resources (risk-)adaptively	EIT, Federated EIT, LSPE	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed (tool settings)
PV-DP-3	Percentage of system services for which privileges can be modified dynamically	Prevent / Avoid	Limit exposure to threat events: Modify privilege restrictions unpredictably	Privilege Restriction: Dynamic Privileges; Unpredictability: Temporal Unpredictability, Contextual Unpredictability	Manage resources (risk-)adaptively	EIT, Federated EIT, LSPE	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed (tool settings)

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
RD-RE-1	Percentage of resources for which an alternative exists	Prevent / Avoid	Limit exposure to threat events: Switch to an alternative resource randomly or in response to a triggering event	Redundancy: Replication	Maintain redundancy	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations), Social / Organizational	Judged
RD-RE-2	Percentage of critical resources for which multiple (more than one) alternatives exist	Prevent / Avoid	Limit exposure to threat events: Switch to an alternative resource randomly or in response to a triggering event	Redundancy: Replication	Maintain redundancy	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations), Social / Organizational	Judged
RD-RE-3	Percentage of processes or services for which an alternative version can be instantiated	Prevent / Avoid	Limit exposure to threat events: Create and switch to an alternative version of process or service randomly or in response to a triggering event	Redundancy: Replication	Maintain redundancy	EIT, LSPE	Engineering	Information / Technical, Cognitive (Cyber Operations)	Judged
SI-PT-1	Average, median, or maximum time required to validate the provenance of mission-critical and system control data	Continue	Ensure that ongoing functioning is correct: Validate provenance of mission-critical and system control data	Substantiated Integrity: Provenance Tracking	Limit the need for trust, Determine ongoing trustworthiness	EIT, Federated EIT, LSPE, CPS, Federated CPS	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
SI-PT-2	Percentage of mission-critical and system control data for which provenance can be validated		Ensure that ongoing functioning is correct: Validate provenance of mission-critical and system control data	Substantiated Integrity: Provenance Tracking	Limit the need for trust, Determine ongoing trustworthiness	EIT, Federated EIT, LSPE, CPS, Federated CPS	Engineering, Tactical Operations, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
SI-PT-3	Average, median, or maximum time required to validate the provenance of security-critical data	Continue	Ensure that ongoing functioning is correct: Validate provenance of mission-critical and system control data	Substantiated Integrity: Provenance Tracking	Limit the need for trust, Determine ongoing trustworthiness	EIT, Federated EIT, LSPE, CPS, Federated CPS	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
SI-PT-4	Percentage of security-critical data for which provenance can be validated	Continue	Ensure that ongoing functioning is correct: Validate provenance of mission-critical and system control data	Substantiated Integrity: Provenance Tracking	Limit the need for trust, Determine ongoing trustworthiness	EIT, Federated EIT, LSPE, CPS, Federated CPS	Engineering, Tactical Operations, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
SI-IC-1	Average, median, or maximum time required to validate the integrity and/or quality of mission-critical data	Continue	Minimize degradation of service delivery: Perform mission damage assessment; Minimize interruptions in service delivery: Perform mission damage assessment; Ensure that ongoing functioning is correct: Validate data integrity / quality to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks	Determine ongoing trustworthiness	EIT, Federated EIT, LSPE, CPS, Federated CPS	Engineering, Tactical Operations, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Measured, Observed, Computed or Derived
SI-IC-2	Percentage of mission-critical data assets for which data integrity / quality can be validated	Continue	Minimize degradation of service delivery: Perform mission damage assessment; Minimize interruptions in service delivery: Perform mission damage assessment; Ensure that ongoing functioning is correct: Validate data integrity / quality to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks	Determine ongoing trustworthiness	EIT, Federated EIT, LSPE, CPS, Federated CPS	Engineering, Tactical Operations, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
SI-IC-3	Average, median, or maximum time required to validate the integrity and/or quality of security-critical data	Continue	Minimize degradation of service delivery: Perform mission damage assessment; Minimize interruptions in service delivery: Perform mission damage assessment; Ensure that ongoing functioning is correct: Validate data integrity / quality to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks	Determine ongoing trustworthiness	EIT, Federated EIT, LSPE, CPS, Federated CPS	Engineering, Tactical Operations, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Measured, Observed, Computed or Derived
SI-IC-4	Number of points in a mission thread where mission-critical data is validated in support of an operation	Continue	Minimize degradation of service delivery: Perform mission damage assessment; Minimize interruptions in service delivery: Perform mission damage assessment; Ensure that ongoing functioning is correct: Validate data integrity / quality to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks	Determine ongoing trustworthiness	EIT, Federated EIT, LSPE, CPS, Federated CPS	Engineering, Tactical Operations, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
SI-IC-5	Percentage of mission-supporting data assets for which data integrity / quality is validated	Constrain	Identify potential damage: Identify potentially corrupted or falsified information	Analytic Monitoring: Monitoring and Damage Assessment; Substantiated Integrity: Integrity Checks	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
SI-IC-6	Data validation includes data format, data types, and ranges [yes/no]	Constrain	Identify potential damage: Identify potentially corrupted or falsified information	Substantiated Integrity: Integrity Checks	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
SI-IC-7	Frequency of hardware / system integrity check	Continue	Ensure that ongoing functioning is correct: Validate hardware / system integrity / behavior to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
SI-IC-8	Hardware / system integrity check performed on operational systems [yes/no]	Continue	Ensure that ongoing functioning is correct: Validate hardware / system integrity / behavior to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
SI-IC-9	Percentage of hardware components to which tamper-evident technologies have been applied	Constrain, Reconstitute	Identify potential damage: Identify potentially faulty, corrupted, or subverted components; Identify damage and untrustworthy resources: Identify damaged, corrupted, or subverted components	Substantiated Integrity: Integrity Checks	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Computed or Derived
SI-BV-1	Average, median, or maximum time required to validate the integrity and/or behavior of mission-critical services or processes	Continue	Ensure that ongoing functioning is correct: Validate software / service integrity / behavior to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks, Behavior Validation	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
SI-BV-2	Percentage of mission-critical applications for which integrity / behavior can be validated	Continue	Ensure that ongoing functioning is correct: Validate software / service integrity / behavior to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks, Behavior Validation	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
SI-BV-3	Average, median, or maximum time required to validate the integrity and/or behavior of security-critical services or processes		Ensure that ongoing functioning is correct: Validate software / service integrity / behavior to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks, Behavior Validation	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
SI-BV-4	Percentage of security-critical systems or system elements (e.g., cryptographic components) for which integrity / behavior can be validated		Ensure that ongoing functioning is correct: Validate software / service integrity / behavior to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks, Behavior Validation	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
SI-BV-5	Number of locations where checks for faulty processes or services occur	Continue, Constrain	Ensure that ongoing functioning is correct: Validate software / service integrity / behavior to ensure it has not been corrupted; Identify potential damage: Identify potentially compromised or faulty processes or services	Analytic Monitoring: Monitoring and Damage Assessment; Substantiated Integrity: Behavior Validation	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed
SI-BV-6	Frequency of check for faulty processes or services [continuously, on demand]	Constrain	Identify potential damage: Identify potentially compromised or faulty processes or services	Analytic Monitoring: Monitoring and Damage Assessment; Substantiated Integrity: Behavior Validation	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed
PA-S1-A1-1	Performance level for "Restrict access to resources based on criticality and sensitivity (i.e., on resource attractiveness to adversaries)"	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: Restrict access to resources based on criticality and sensitivity (i.e., on resource attractiveness to adversaries)	Privilege Restriction: Trust-Based Privilege Management, Attribute-Based Usage Restriction; Segmentation: Predefined Segmentation	Control visibility and use	All	Engineering, Investment / Programmatic	Cognitive (Cyber Operations)	Judged

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PA-S1-A1-2	Percentage of cyber resources to which access is controlled based on criticality	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: Restrict access to resources based on criticality and sensitivity	Privilege Restriction: Trust-Based Privilege Management, Attribute-Based Usage Restriction; Segmentation: Predefined Segmentation	Control visibility and use	EIT, LSPE, PIT, CPS	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Judged, Measured, Computed or Derived
PA-S1-A1-3	Percentage of cyber resources to which access is controlled based on sensitivity	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: Restrict access to resources based on criticality and sensitivity	Privilege Restriction: Trust-Based Privilege Management, Attribute-Based Usage Restriction; Segmentation: Predefined Segmentation	Control visibility and use	EIT, LSPE, PIT, CPS	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Judged, Measured, Computed or Derived
PA-S1-A1-4	Percentage of users with privileged / administrator access	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: Restrict access to resources based on criticality and sensitivity	Privilege Restriction: Trust-Based Privilege Management, Attribute-Based Usage Restriction	Limit the need for trust	EIT, LSPE, PIT, CPS	Tactical Operations, Investment / Programmatic	Information / Technical	
PA-S1-A1-5	Percentage of [administrative, operational] activities [procedurally, Information / Technically] enforced by 2-person controls	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: Restrict access to resources based on criticality and sensitivity	Privilege Restriction: Trust-Based Privilege Management, Attribute-Based Usage Restriction	Limit the need for trust	EIT, LSPE, PIT, CPS	Tactical Operations, Investment / Programmatic	Information / Technical	Judged; Measured, Observed
PA-S1-A2-1	Percentage of users for which behaviors are restricted based on assigned degree of trust	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: Restrict behaviors of users and cyber entities based on degree of trust	Privilege Restriction: Trust-Based Privilege Management, Attribute-Based Usage Restriction	Limit the need for trust	EIT, LSPE, PIT, CPS	Tactical Operations, Investment / Programmatic	Information / Technical	Judged; Measured, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PA-S1-A2-2	Percentage of types of cyber entities for which behaviors are restricted based on assigned degree of trust	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: 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	Limit the need for trust	EIT, LSPE, CPS, PIT	Tactical Operations, Investment / Programmatic	Information / Technical	Judged; Measured, Observed
PA-S1-A3-1	Percentage of cyber resources which can be placed in a single enclave	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: Enforce clear boundaries on sets of cyber resources	Segmentation: Predefined Segmentation, Realignment: Purposing	Contain and exclude behaviors	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Judged; Measured, Observed
PA-S1-A3-2	Percentage of cyber resources which have been placed in a single enclave	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: Enforce clear boundaries on sets of cyber resources	Segmentation: Predefined Segmentation, Realignment: Purposing	Contain and exclude behaviors	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Judged; Measured, Observed
PA-S1-A3-3	Percentage of cyber resources which can be discovered, accessed or used, or otherwise reached from another enclave	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: Enforce clear boundaries on sets of cyber resources	Segmentation: Predefined Segmentation, Realignment: Purposing	Contain and exclude behaviors	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Measured, Observed (network mapping / resource inventory tools)
PA-S1-A3-4	Number of dedicated operational enclaves defined	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: Enforce clear boundaries on sets of cyber resources	Segmentation: Predefined Segmentation, Realignment: Purposing	Contain and exclude behaviors	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Judged
PA-S1-A3-5	Number of dedicated administrative enclaves defined	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: Enforce clear boundaries on sets of cyber resources	Segmentation: Predefined Segmentation, Realignment: Purposing	Contain and exclude behaviors	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Judged
PA-S1-A3-6	Number of dedicated security/audit enclaves defined	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: Enforce clear boundaries on sets of cyber resources	Segmentation: Predefined Segmentation, Realignment: Purposing	Contain and exclude behaviors	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Judged

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PA-S1-A3-7	Percentage of enclaves associated with a single operational function	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: Enforce clear boundaries on sets of cyber resources	Segmentation: Predefined Segmentation, Realignment: Purposing	Contain and exclude behaviors	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Judged
PA-S1-A4-1	Percentage of critical cyber resources to which multiple defenses are applied	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: Enforce clear boundaries on sets of cyber resources	Coordinated Protection: Calibrated Defense-in-Depth, Orchestration	Layer defenses and partition resources	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Judged
PA-S1-A5-1	Percentage of external communications which are encrypted	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: Protect data in different states (e.g., at rest, in transit, in processing)	Deception: Obfuscation	Control visibility and use	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Measured (network analysis tools)
PA-S1-A5-2	Percentage of internal communications which are encrypted	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: Protect data in different states (e.g., at rest, in transit, in processing)	Deception: Obfuscation	Control visibility and use	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Measured (network analysis tools)
PA-S1-A5-3	Percentage of information stores which are encrypted	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: Protect data in different states (e.g., at rest, in transit, in processing)	Deception: Obfuscation	Control visibility and use	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Measured (analysis tools)
PA-S1-A5-4	Percentage of processing which is encrypted or obfuscated	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: Protect data in different states (e.g., at rest, in transit, in processing)	Deception: Obfuscation	Control visibility and use	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Measured (analysis tools)

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PA-S1-A5-5	Strength of encryption mechanism for [external communications | internal communications | information stores | processing]	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: Protect data in different states (e.g., at rest, in transit, in processing)	Deception: Obfuscation	Control visibility and use	EIT, LSPE, CPS, PIT	Engineering, Investment / Programmatic	Information / Technical	Judged
PA-S2-A1-1	Percentage of configuration parameters for which allowable ranges have been defined	Prevent / Avoid	Limit exposure to threat events: Identify and implement a set of change parameters	Coordinated Protection: Consistency Analysis	Limit the need for trust	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Judged
PA-S2-A1-2	Percentage of CCoAs which make changes within allowable ranges	Prevent / Avoid	Limit exposure to threat events: Identify and implement a set of change parameters	Coordinated Protection: Consistency Analysis	Limit the need for trust	EIT, LSPE, CPS, PIT	COA Analysis, Investment / Programmatic	Information / Technical	Judged
PA-S2-A1-3	Percentage of automated change mechanisms for which changes can be restricted to allowable ranges	Prevent / Avoid	Limit exposure to threat events: Identify and implement a set of change parameters	Coordinated Protection: Consistency Analysis	Limit the need for trust	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Information / Technical	Judged
PA-S2-A1-4	Percentage of change parameters permitted to control unpredictability, outside of a schedule	Prevent / Avoid	Limit exposure to threat events: Identify and implement a set of change parameters	Coordinated Protection: Consistency Analysis	Limit the need for trust	EIT, LSPE, CPS, PIT	Tactical Operations, Investment / Programmatic	Information / Technical	Judged
PA-S2-A2-1	Percentage of resources for which an alternative exists for which switching is performed	Prevent / Avoid, Constrain	Limit exposure to threat events: Switch to an alternative resource randomly or in response to a triggering event; Change or remove resources and how they are used to limit future or further damage: Switch to an alternative resource	Adaptive Response: Dynamic Reallocation; Redundancy: Replication	Change or disrupt the attack surface	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Judged

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PA-S2-A2-2	Percentage of resources switches enabled by random vs. triggered events	Prevent / Avoid	Limit exposure to threat events: Switch to an alternative resource randomly or in response to a triggering event	Adaptive Response: Dynamic Reallocation; Redundancy: Replication; Unpredictability: Contextual Unpredictability, Temporal Unpredictability	Change or disrupt the attack surface	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Judged
PA-S2-A2-3	Average time to complete the switching process (latency or lag)	Prevent / Avoid, Constrain	Limit exposure to threat events: Switch to an alternative resource randomly or in response to a triggering event; Change or remove resources and how they are used to limit future or further damage: Switch to an alternative resource	Adaptive Response: Dynamic Reallocation; Redundancy: Replication; Unpredictability: Contextual Unpredictability, Temporal Unpredictability	Change or disrupt the attack surface	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Measured, Observed
PA-S2-A2-4	Average frequency of switches to an alternative resource per unit time	Prevent / Avoid, Constrain	Limit exposure to threat events: Switch to an alternative resource randomly or in response to a triggering event; Change or remove resources and how they are used to limit future or further damage: Switch to an alternative resource	Adaptive Response: Dynamic Reallocation; Redundancy: Replication; Unpredictability: Contextual Unpredictability, Temporal Unpredictability	Change or disrupt the attack surface	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Measured, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PA-S2-A3-1	Percentage of processes or services for which an alternative version can be instantiated for which instantiation is performed	Prevent / Avoid	Limit exposure to threat events: 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	Maintain redundancy, Change or disrupt the attack surface	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Judged
PA-S2-A3-2	Average time to complete the process of instantiating and switching to an alternative version of a process or service	Prevent / Avoid	Limit exposure to threat events: 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	Maintain redundancy, Change or disrupt the attack surface	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Information / Technical	Measured, Observed, Computed or Derived
PA-S2-A3-3	Average frequency of switches to an alternative version of a process or service per unit time	Prevent / Avoid	Limit exposure to threat events: 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	Maintain redundancy, Change or disrupt the attack surface	EIT, LSPE, CPS, PIT	Tactical Operations	Information / Technical	Measured, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PA-S2-A4-1	Percentage of resources for which configuration changes can be made	Prevent / Avoid, Constrain	Limit exposure to threat events: Reconfigure components and services randomly or in response to a triggering event; Change or remove resources and how they are used to limit future or further damage: Reconfigure components and services	Adaptive Response: Dynamic Reconfiguration	Manage resources (risk-) adaptively	EIT, LSPE, CPS, PIT	Engineering, Investment / Programmatic	Information / Technical	Judged, Computed or Derived
PA-S2-A4-2	Percentage of resources to which configuration changes can be made randomly or in response to a triggering event	Prevent / Avoid, Constrain	Limit exposure to threat events: Reconfigure components and services randomly or in response to a triggering event; Change or remove resources and how they are used to limit future or further damage: Reconfigure components and services	Adaptive Response: Dynamic Reconfiguration; Unpredictability: Contextual Unpredictability, Temporal Unpredictability	Manage resources (risk-) adaptively	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Information / Technical	Judged, Measured, Observed
PA-S2-A4-3	Percentage of resources to which configuration changes can be made dynamically for which changes are made randomly or in response to a triggering event	Prevent / Avoid, Constrain	Limit exposure to threat events: Reconfigure components and services randomly or in response to a triggering event; Change or remove resources and how they are used to limit future or further damage: Reconfigure components and services	Adaptive Response: Dynamic Reconfiguration; Unpredictability: Contextual Unpredictability, Temporal Unpredictability	Manage resources (risk-) adaptively	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Information / Technical	Measured, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PA-S2-A4-4	Average time to complete the dynamic reconfiguration process	Prevent / Avoid, Constrain	Limit exposure to threat events: Reconfigure components and services randomly or in response to a triggering event; Change or remove resources and how they are used to limit future or further damage: Reconfigure components and services	Adaptive Response: Dynamic Reconfiguration; Segmentation: Dynamic Segmentation & Isolation	Manage resources (risk-) adaptively	EIT, LSPE, CPS, PIT	Tactical Operations	Information / Technical	Measured, Observed, Computed or Derived
PA-S2-A4-5	Frequency of configuration changes per unit time	Prevent / Avoid, Constrain	Limit exposure to threat events: Reconfigure components and services randomly or in response to a triggering event; Change or remove resources and how they are used to limit future or further damage: Reconfigure components and services	Adaptive Response: Dynamic Reconfiguration; Segmentation: Dynamic Segmentation & Isolation; Unpredictability: Contextual Unpredictability, Temporal Unpredictability	Manage resources (risk-) adaptively	EIT, LSPE, CPS, PIT	Tactical Operations	Information / Technical	Measured, Observed, Computed or Derived
PA-S2-A5-1	Percentage of resources which can be relocated virtually which are relocated	Prevent / Avoid, Constrain	Limit exposure to threat events: Dynamically relocate processing randomly or in response to a triggering event; Change or remove resources and how they are used to limit future or further damage: Dynamically relocate processing	Adaptive Response: Dynamic Reconfiguration; Dynamic Positioning: Asset Mobility, Functional Relocation of Cyber Resources; Unpredictability: Contextual Unpredictability, Temporal Unpredictability	Make resources location-versatile	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Information / Technical	Judged; Measured, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PA-S2-A5-2	Percentage of resources which can be relocated physically which are relocated	Prevent / Avoid, Constrain	Limit exposure to threat events: Dynamically relocate processing randomly or in response to a triggering event; Change or remove resources and how they are used to limit future or further damage: Dynamically relocate processing	Adaptive Response: Dynamic Reconfiguration; Dynamic Positioning: Asset Mobility, Functional Relocation of Cyber Resources; Unpredictability: Contextual Unpredictability, Temporal Unpredictability	Make resources location-versatile	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Judged; Measured, Observed
PA-S2-A5-3	Frequency of relocation events per unit time	Prevent / Avoid, Constrain	Limit exposure to threat events: Dynamically relocate processing randomly or in response to a triggering event; Change or remove resources and how they are used to limit future or further damage: Dynamically relocate processing	Adaptive Response: Dynamic Reconfiguration; Dynamic Positioning: Asset Mobility, Functional Relocation of Cyber Resources; Unpredictability: Contextual Unpredictability, Temporal Unpredictability	Make resources location-versatile	EIT, LSPE, CPS, PIT	Tactical Operations	Information / Technical	Measured, Observed, Computed or Derived
PA-S2-A6-1	Percentage of communications paths to which lifespan conditions are applied	Prevent / Avoid	Limit exposure to threat events: Retain resources in an active or "live" state for a limited lifespan	Non-Persistence: Non-Persistent Connectivity	Maximize transience	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Information / Technical, Cognitive (Cyber Operations)	Judged; Measured, Observed
PA-S2-A6-2	Percentage of mission services to which lifespan conditions are applied	Prevent / Avoid	Limit exposure to threat events: Retain resources in an active or "live" state for a limited lifespan	Non-Persistence: Non-Persistent Services	Maximize transience	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Information / Technical, Cognitive (Cyber Operations)	Judged; Measured, Observed
PA-S2-A6-3	Percentage of supporting services to which lifespan conditions are applied	Prevent / Avoid	Limit exposure to threat events: Retain resources in an active or "live" state for a limited lifespan	Non-Persistence: Non-Persistent Services	Maximize transience	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Information / Technical, Cognitive (Cyber Operations)	Judged; Measured, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PA-S2-A6-4	Percentage of information resources to which lifespan conditions are applied	Prevent / Avoid	Limit exposure to threat events: Retain resources in an active or "live" state for a limited lifespan	Non-Persistence: Non-Persistent Information	Maximize transience	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Information / Technical, Cognitive (Cyber Operations)	Judged; Measured, Observed
PA-S2-A6-5	Percentage of lifespan conditions determined based on threat intelligence or known adversarial TTPs	Prevent / Avoid	Limit exposure to threat events: Retain resources in an active or "live" state for a limited lifespan	Non-Persistence: Non-Persistent Services, Non-Persistent Connectivity, Non-Persistent Information	Maximize transience	EIT, LSPE, CPS, PIT	Tactical Operations	Information / Technical, Cognitive (Cyber Operations)	Judged
PA-S2-A6-6	Maximum or average lifespan of a communications path	Prevent / Avoid, Constrain	Limit exposure to threat events: Retain resources in an active or "live" state for a limited lifespan; Change or remove resources and how they are used to limit future or further damage: Retain resources for a limited lifespan	Non-Persistence: Non-Persistent Services, Non-Persistent Connectivity, Non-Persistent Information	Maximize transience	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
PA-S2-A6-7	Maximum or average lifespan of a mission service	Prevent / Avoid, Constrain	Limit exposure to threat events: Retain resources in an active or "live" state for a limited lifespan; Change or remove resources and how they are used to limit future or further damage: Retain resources for a limited lifespan	Non-Persistence: Non-Persistent Services, Non-Persistent Connectivity, Non-Persistent Information	Maximize transience	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PA-S2-A6-8	Maximum or average lifespan of a supporting service	Prevent / Avoid, Constrain	Limit exposure to threat events: Retain resources in an active or "live" state for a limited lifespan; Change or remove resources and how they are used to limit future or further damage: Retain resources for a limited lifespan	Non-Persistence: Non-Persistent Services, Non-Persistent Connectivity, Non-Persistent Information	Maximize transience	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
PA-S2-A6-9	Maximum or average lifespan of an information resource	Prevent / Avoid, Constrain	Limit exposure to threat events: Retain resources in an active or "live" state for a limited lifespan; Change or remove resources and how they are used to limit future or further damage: Retain resources for a limited lifespan	Non-Persistence: Non-Persistent Services, Non-Persistent Connectivity, Non-Persistent Information	Maximize transience	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
PA-S2-A7-1	Amount of information which can be retrieved or reconstructed by a Red Team after an information resource is deleted	Prevent / Avoid, Constrain	Limit exposure to threat events, Change or remove resources and how they are used to limit future or further damage: 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	Layer defenses and partition resources, Maximize transience	EIT, LSPE, CPS, PIT	Tactical Operations	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PA-S2-A7-2	Amount of [mission critical, sensitive] information which can be retrieved or reconstructed by a Red Team after a service is moved or terminated	Prevent / Avoid, Constrain	Limit exposure to threat events, Change or remove resources and how they are used to limit future or further damage: 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	Layer defenses and partition resources, Maximize transience	EIT, LSPE, CPS, PIT	Tactical Operations	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
PA-S2-A8-1	Percentage of mission-critical cyber resources which can be discovered or reached from each enclave, sub-system, or network nodes	Prevent / Avoid	Limit exposure to threat events: Separate cyber resources based on criticality and/or sensitivity	Segmentation: Predefined Segmentation	Control visibility and use	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Measured, Observed (network mapping / resource inventory tools)
PA-S2-A8-2	Percentage of high-sensitivity information stores which can be discovered or reached from all sub-systems or network nodes	Prevent / Avoid	Limit exposure to threat events: Separate cyber resources based on criticality and/or sensitivity	Segmentation: Predefined Segmentation	Control visibility and use	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Measured, Observed (network mapping / resource inventory tools)
PA-S2-A9-1	Percentage of high-sensitivity or high-criticality information stores which are fragmented across multiple locations	Prevent / Avoid	Limit exposure to threat events: Split or distribute cyber resources across multiple locations to avoid creating high-value targets	Dynamic Positioning: Fragmentation, Distributed Functionality	Make resources location-versatile	EIT, Federated EIT, LSPE	Engineering, Administrative / Management, Tactical Operations, Investment / Programmatic	Information / Technical	Judged, Computed or Derived
PA-S2-A9-2	Number of geographically diverse locations included in the fragmentation set	Prevent / Avoid	Limit exposure to threat events: Split or distribute cyber resources across multiple locations to avoid creating high-value targets	Dynamic Positioning: Fragmentation	Make resources location-versatile	EIT, Federated EIT, LSPE	Engineering, Administrative / Management, Tactical Operations, Investment / Programmatic	Information / Technical	Judged

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PA-S2-A9-3	Percentage of mission-critical functions which are executed by distributed rather than centralized services	Prevent / Avoid	Limit exposure to threat events: Split or distribute cyber resources across multiple locations to avoid creating high-value targets	Dynamic Positioning: Distributed Functionality	Make resources location-versatile	EIT, Federated EIT, LSPE	Engineering, Administrative / Management, Tactical Operations, Investment / Programmatic	Information / Technical	Judged
PA-S2-A10-1	Percentage of cyber resources for which privileges can be modified randomly for which privileges are modified randomly	Prevent / Avoid	Limit exposure to threat events: Modify privilege restrictions unpredictably	Privilege Restriction: Dynamic Privileges; Unpredictability: Temporal Unpredictability, Contextual Unpredictability	Limit the need for trust, Contain and exclude behaviors, Make the effects of deception and unpredictability user-transparent	EIT, Federated EIT, LSPE	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed (tool settings)
PA-S2-A10-2	Percentage of users for whom privileges can be modified randomly whose privileges are modified randomly	Prevent / Avoid	Limit exposure to threat events: Modify privilege restrictions unpredictably	Privilege Restriction: Dynamic Privileges; Unpredictability: Temporal Unpredictability, Contextual Unpredictability	Limit the need for trust, Contain and exclude behaviors, Make the effects of deception and unpredictability user-transparent	EIT, Federated EIT, LSPE	Engineering, Administrative / Management, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed (tool settings)
PA-S2-A10-3	Percentage of system services for which privileges can be modified randomly for which privileges are modified randomly	Prevent / Avoid	Limit exposure to threat events: Modify privilege restrictions unpredictably	Privilege Restriction: Dynamic Privileges; Unpredictability: Temporal Unpredictability, Contextual Unpredictability	Limit the need for trust, Contain and exclude behaviors, Make the effects of deception and unpredictability user-transparent	EIT, Federated EIT, LSPE	Engineering, Administrative / Management, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured or Observed (tool settings)
PA-S3-A1-1	Percentage of sensitive data stores that are encrypted	Prevent / Avoid	Decrease the adversary's perceived benefits: Conceal resources an adversary might find attractive	Deception: Obfuscation	Control visibility and use	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Judged,Measured, Observed (network mapping / resource inventory tools)
PA-S3-A1-2	Strength of encryption used to protect sensitive data stores	Prevent / Avoid	Decrease the adversary's perceived benefits: Conceal resources an adversary might find attractive	Deception: Obfuscation	Control visibility and use	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Investment / Programmatic	Information / Technical	Judged

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PA-S3-A1-3	Percentage of data streams used for sensitive data that are encrypted	Prevent / Avoid	Decrease the adversary's perceived benefits: Conceal resources an adversary might find attractive	Deception: Obfuscation	Control visibility and use	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical	Judged, Measured or Observed (network mapping / resource inventory tools)
PA-S3-A1-4	Strength of encryption used to protect sensitive data streams	Prevent / Avoid	Decrease the adversary's perceived benefits: Conceal resources an adversary might find attractive	Deception: Obfuscation	Control visibility and use	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Investment / Programmatic	Information / Technical	Judged
PA-S3-A1-5	Time for a Red Team to identify which critical resources are involved in mission processing	Prevent / Avoid	Decrease the adversary's perceived benefits: Conceal resources an adversary might find attractive	Deception: Obfuscation	Control visibility and use	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed
PA-S3-A2-1	Number of external venues in which misleading or false information is presented	Prevent / Avoid	Decrease the adversary's perceived benefits: Present misleading information about information, resources, and capabilities	Deception: Dissimulation, Misdirection	Control visibility and use	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Tactical Operations, Investment / Programmatic	Cognitive (Cyber Operations)	Judged, Observed
PA-S3-A2-2	Number of internal venues in which misleading or false information is presented	Prevent / Avoid	Decrease the adversary's perceived benefits: Present misleading information about information, resources, and capabilities	Deception: Dissimulation, Misdirection	Control visibility and use	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Tactical Operations, Investment / Programmatic	Cognitive (Cyber Operations)	Judged
PA-S3-A2-3	Frequency of updates to misleading or false information	Prevent / Avoid	Decrease the adversary's perceived benefits: Present misleading information about information, resources, and capabilities	Deception: Dissimulation, Misdirection	Control visibility and use	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Tactical Operations, Investment / Programmatic	Cognitive (Cyber Operations)	Judged, Measured, Observed (tool settings)

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PA-S3-A2-4	Time since last update of misleading or false information	Prevent / Avoid	Decrease the adversary's perceived benefits: Present misleading information about information, resources, and capabilities	Deception: Dissimulation, Misdirection	Control visibility and use	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Tactical Operations, Investment / Programmatic	Cognitive (Cyber Operations)	Judged, Measured, Observed
PA-S4-A1-1	Percentage of resources to which changes to privileges and access / usage restrictions can be made dynamically	Prevent / Avoid	Modify configurations based on threat intelligence: 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	Manage resources (risk-) adaptively	EIT, LSPE, CPS	Engineering, Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed
PA-S4-A1-2	Percentage of resources for which changes to privileges and access / usage restrictions are made dynamically+B206 in response to I&W	Prevent / Avoid	Modify configurations based on threat intelligence: 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	Manage resources (risk-) adaptively	EIT, LSPE, CPS	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed
PA-S4-A1-3	Time to propagate modifications to privileges and access / usage restrictions to all resources which should be affected	Prevent / Avoid	Modify configurations based on threat intelligence: 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	Manage resources (risk-) adaptively	EIT, LSPE, CPS	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PA-S4-A2-1	Time since last scrub of privilege definition and assignment	Prevent / Avoid	Modify configurations based on threat intelligence: Coordinate definition and assignment of privileges to eliminate opportunities for privilege escalation	Coordinated Protection: Consistency Analysis; Privilege Restriction: Trust-Based Privilege Management, Dynamic Privileges	Make resources location-versatile	EIT, LSPE, CPS	Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed
PA-S4-A2-2	Frequency of review of privileged definition and assignment	Prevent / Avoid	Modify configurations based on threat intelligence: Coordinate definition and assignment of privileges to eliminate opportunities for privilege escalation	Coordinated Protection: Consistency Analysis; Privilege Restriction: Trust-Based Privilege Management, Dynamic Privileges	Make resources location-versatile	EIT, LSPE, CPS	Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed
PA-S4-A2-3	Random reviews performed on privilege definitions / assignments [yes/no]	Prevent / Avoid	Modify configurations based on threat intelligence: Coordinate definition and assignment of privileges to eliminate opportunities for privilege escalation	Coordinated Protection: Consistency Analysis; Privilege Restriction: Trust-Based Privilege Management, Dynamic Privileges	Make resources location-versatile	EIT, LSPE, CPS	Administrative / Management, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed
PA-S4-A2-4	Number of distinct privileges which can be assigned to an individual or process	Prevent / Avoid	Modify configurations based on threat intelligence: Coordinate definition and assignment of privileges to eliminate opportunities for privilege escalation	Privilege Restriction: Trust-Based Privilege Management, Dynamic Privileges	Make resources location-versatile	EIT, LSPE, CPS	Administrative / Management, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed
PA-S4-A2-5	Complexity of the set of privileges, when represented as a partially directed graph	Prevent / Avoid	Modify configurations based on threat intelligence: Coordinate definition and assignment of privileges to eliminate opportunities for privilege escalation	Privilege Restriction: Trust-Based Privilege Management, Dynamic Privileges	Make resources location-versatile	EIT, LSPE, CPS	Administrative / Management, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PA-S4-A2-6	Percentage of users assigned to each privilege	Prevent / Avoid	Modify configurations based on threat intelligence: Coordinate definition and assignment of privileges to eliminate opportunities for privilege escalation	Privilege Restriction: Trust-Based Privilege Management, Dynamic Privileges	Make resources location-versatile	EIT, LSPE, CPS	Administrative / Management, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed
PA-S4-A2-7	Percentage of users with access to [read, modify] critical resources or sensitive information	Prevent / Avoid	Modify configurations based on threat intelligence: Coordinate definition and assignment of privileges to eliminate opportunities for privilege escalation	Privilege Restriction: Trust-Based Privilege Management, Dynamic Privileges	Make resources location-versatile	EIT, LSPE, CPS	Administrative / Management, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed
PR-S1-A1-1	Percentage of cyber resources which can be defended by automated CCoAs	Prepare	Create and maintain cyber courses of action: Define and implement automated CCoAs	Adaptive Response: Adaptive Management; Coordinated Protection: Orchestration	Manage resources (risk-) adaptively	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Investment / Programmatic, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged
PR-S1-A1-2	Percentage of identified threat types, categories of threat actions, or TTPs [with reference to an identified threat model] for which automated CCoAs are defined	Prepare	Create and maintain cyber courses of action: Define and implement automated CCoAs	Adaptive Response: Adaptive Management; Coordinated Protection: Orchestration	Manage resources (risk-) adaptively	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Investment / Programmatic, COA Analysis	Cognitive (Cyber Operations)	Judged
PR-S1-A2-1	Number of CCoAs documented in the organization's cyber playbook	Prepare	Create and maintain cyber courses of action: Define / maintain a cyber playbook containing realistic CCoAs	Coordinated Protection: Consistency Analysis, Orchestration	Manage resources (risk-) adaptively	EIT, LSPE, CPS	Investment / Programmatic, COA Analysis	Cognitive (Cyber Operations)	Judged

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PR-S1-A2-2	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	Prepare	Create and maintain cyber courses of action: Define / maintain a cyber playbook containing realistic CCoAs	Coordinated Protection: Consistency Analysis, Orchestration	Manage resources (risk-) adaptively	EIT, LSPE, CPS	Investment / Programmatic, COA Analysis	Cognitive (Cyber Operations)	Judged
PR-S1-A2-3	Percentage of potential classes of cyber effects addressed by at least one CCoA in the cyber playbook	Prepare	Create and maintain cyber courses of action: Define / maintain a cyber playbook containing realistic CCoAs	Coordinated Protection: Consistency Analysis, Orchestration	Manage resources (risk-) adaptively	EIT, LSPE, CPS	Investment / Programmatic, COA Analysis	Cognitive (Cyber Operations)	Judged
PR-S1-A2-4	Time since last update of the organization's cyber playbook	Prepare	Create and maintain cyber courses of action: Define / maintain a cyber playbook containing realistic CCoAs	Coordinated Protection: Consistency Analysis, Orchestration	Manage resources (risk-) adaptively	EIT, LSPE, CPS	Investment / Programmatic, COA Analysis	Cognitive (Cyber Operations)	Judged
PR-S1-A2-5	Frequency of CCoA review/updates	Prepare	Create and maintain cyber courses of action: Define / maintain a cyber playbook containing realistic CCoAs	Coordinated Protection: Consistency Analysis, Orchestration	Manage resources (risk-) adaptively	EIT, LSPE, CPS	Investment / Programmatic, COA Analysis	Cognitive (Cyber Operations)	Judged
PR-S1-A3-1	Percentage of CCoAs for which MOEs are defined	Prepare	Create and maintain cyber courses of action: Track effectiveness of CCoAs and adapt as necessary	Adaptive Response: Adaptive Management; Coordinated Protection: Consistency Analysis, Orchestration	Manage resources (risk-) adaptively	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Investment / Programmatic, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PR-S1-A3-2	Percentage of CCoAs for which MOEs are tracked	Prepare	Create and maintain cyber courses of action: Track effectiveness of CCoAs and adapt as necessary	Adaptive Response: Adaptive Management; Coordinated Protection: Consistency Analysis, Orchestration	Manage resources (risk-) adaptively	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Investment / Programmatic, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged
PR-S1-A3-3	Average time between the exercise of a CCoA and its update	Prepare	Create and maintain cyber courses of action: Track effectiveness of CCoAs and adapt as necessary	Adaptive Response: Adaptive Management; Coordinated Protection: Consistency Analysis, Orchestration	Manage resources (risk-) adaptively	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Investment / Programmatic, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged
PR-S1-A3-4	For each possible effect on threat event, the number of CCoAs which are expected to have that effect	Prepare	Create and maintain cyber courses of action: Track effectiveness of CCoAs and adapt as necessary	Adaptive Response: Adaptive Management; Coordinated Protection: Consistency Analysis, Orchestration	Manage resources (risk-) adaptively	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Investment / Programmatic, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged
PR-S2-A1-1	Percentage of cyber resources which are backed up	Prepare	Create and maintain cyber courses of action: Back up data needed to restore or reconstitute mission and supporting functionality	Redundancy: Protected Backup and Restore	Maintain redundancy	EIT, LSPE, CPS	Tactical Operations, Administrative / Management, Investment / Programmatic	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed
PR-S2-A1-2	Percentage of cyber resources which are in hot backups	Prepare	Create and maintain cyber courses of action: Back up data needed to restore or reconstitute mission and supporting functionality	Redundancy: Protected Backup and Restore	Maintain redundancy	EIT, LSPE, CPS	Tactical Operations, Administrative / Management, Investment / Programmatic	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PR-S2-A1-3	Percentage of cyber resources which are backed up into cold / archival storage	Prepare	Create and maintain cyber courses of action: Back up data needed to restore or reconstitute mission and supporting functionality	Redundancy: Protected Backup and Restore	Maintain redundancy	EIT, LSPE, CPS	Tactical Operations, Administrative / Management, Investment / Programmatic	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed
PR-S2-A1-4	Time since restoration / reconstitution processes were last exercised	Prepare	Create and maintain cyber courses of action: Back up data needed to restore or reconstitute mission and supporting functionality	Redundancy: Protected Backup and Restore	Maintain redundancy	EIT, LSPE, CPS	Tactical Operations, Administrative / Management, Investment / Programmatic	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed
PR-S2-A1-5	Average time to restore	Prepare	Create and maintain cyber courses of action: Back up data needed to restore or reconstitute mission and supporting functionality	Redundancy: Protected Backup and Restore	Maintain redundancy	EIT, LSPE, CPS	Tactical Operations, Administrative / Management, Investment / Programmatic	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed
PR-S2-A1-6	Average time to back up	Prepare	Create and maintain cyber courses of action: Back up data needed to restore or reconstitute mission and supporting functionality	Redundancy: Protected Backup and Restore	Maintain redundancy	EIT, LSPE, CPS	Tactical Operations, Administrative / Management, Investment / Programmatic	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed
PR-S2-A1-7	Frequency of backup	Prepare	Create and maintain cyber courses of action: Back up data needed to restore or reconstitute mission and supporting functionality	Redundancy: Protected Backup and Restore	Maintain redundancy	EIT, LSPE, CPS	Tactical Operations, Administrative / Management, Investment / Programmatic	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed
PR-S2-A2-1	Percentage of those CCoAs for which alternative resources (e.g., at a standby site) identified in the CCoA are available	Prepare	Maintain the resources needed to execute cyber courses of action: Pre-position resources to support CCoAs	Coordinated Protection: Calibrated Defense-in-Depth, Orchestration; Redundancy: Surplus Capacity, Replication	Maintain redundancy	EIT, LSPE, CPS	Administrative / Management, Investment / Programmatic, COA Analysis	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PR-S2-A2-2	Elapsed time since a spot check of the availability of alternate resources for each CCoA has been performed	Prepare	Maintain the resources needed to execute cyber courses of action: Pre-position resources to support CCoAs	Coordinated Protection: Calibrated Defense-in-Depth, Orchestration; Redundancy: Surplus Capacity, Replication	Maintain redundancy	EIT, LSPE, CPS	Tactical Operations, Administrative / Management, COA Analysis	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed
PR-S2-A2-3	Percentage of those CCoAs for which staff identified in the CCoA have been trained in their responsibilities with respect to the CCoA	Prepare	Maintain the resources needed to execute cyber courses of action: Pre-position resources to support CCoAs	Coordinated Protection: Calibrated Defense-in-Depth, Orchestration; Redundancy: Surplus Capacity, Replication	Maintain redundancy	EIT, LSPE, CPS	Tactical Operations, Administrative / Management, COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations), Social / Organizational	Computed or Derived, Measured, Observed
PR-S2-A2-4	Average time since last staff training with respect to the CCoA	Prepare	Maintain the resources needed to execute cyber courses of action	Coordinated Protection: Calibrated Defense-in-Depth, Orchestration; Redundancy: Surplus Capacity, Replication	Maintain redundancy	EIT, LSPE, CPS	Tactical Operations, Administrative / Management, COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations), Social / Organizational	Computed or Derived, Measured, Observed
PR-S2-A3-1	Percentage of mission-essential software (with supporting configuration data) for which a gold copy exists	Prepare	Maintain the resources needed to execute cyber courses of action: Maintain gold copies of mission-essential software and configuration data	Redundancy: Protected Backup and Restore	Maintain redundancy	EIT, LSPE, CPS	Engineering, Tactical Operations, Administrative / Management	Information / Technical	Judged, Computed or Derived, Observed
PR-S2-A3-2	Time since last update of the gold copy	Prepare	Maintain the resources needed to execute cyber courses of action: Maintain gold copies of mission-essential software and configuration data	Redundancy: Protected Backup and Restore	Maintain redundancy	EIT, LSPE, CPS	Tactical Operations, Administrative / Management	Information / Technical, Cognitive (Cyber Operations)	Measured, Observed
PR-S2-A3-3	Time since last validation of the gold copy	Prepare	Maintain the resources needed to execute cyber courses of action: Maintain gold copies of mission-essential software and configuration data	Redundancy: Protected Backup and Restore	Maintain redundancy	EIT, LSPE, CPS	Tactical Operations, Administrative / Management	Information / Technical, Cognitive (Cyber Operations)	Measured, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PR-S2-A3-4	Time taken between system updates and generation of gold copy	Prepare	Maintain the resources needed to execute cyber courses of action: Maintain gold copies of mission-essential software and configuration data	Redundancy: Protected Backup and Restore	Maintain redundancy	EIT, LSPE, CPS	Tactical Operations, Administrative / Management	Information / Technical, Cognitive (Cyber Operations)	Measured, Observed
PR-S2-A4-1	Percentage of information or processing resources which can be snapshot, expunged, and restored to a known good state	Prepare	Maintain the resources needed to execute cyber courses of action: Provide mechanisms and/or procedures for snapshotting or otherwise capturing, and then restoring, state	Analytic Monitoring: Malware and Forensic Analysis	Manage resources (risk-) adaptively	EIT, LSPE, CPS	Tactical Operations, Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived, Observed
PR-S2-A4-2	Time since snapshotting and restoration mechanisms have been last exercised	Prepare	Maintain the resources needed to execute cyber courses of action: Provide mechanisms and/or procedures for snapshotting or otherwise capturing, and then restoring, state	Analytic Monitoring: Malware and Forensic Analysis	Manage resources (risk-) adaptively	EIT, LSPE, CPS	Tactical Operations, Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Measured or Observed
PR-S2-A4-3	Can snapshot be performed live [yes/no]	Prepare	Maintain the resources needed to execute cyber courses of action: Provide mechanisms and/or procedures for snapshotting or otherwise capturing, and then restoring, state	Analytic Monitoring: Malware and Forensic Analysis	Manage resources (risk-) adaptively	EIT, LSPE, CPS	Tactical Operations, Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PR-S2-A5-1	Percentage of mission-critical hardware components for which protected alternates are maintained	Prepare	Maintain the resources needed to execute cyber courses of action: Maintain multiple protected instances of hardware	Diversity: Supply Chain Diversity; Redundancy: Replication	Maintain redundancy	EIT, LSPE, CPS	Engineering, Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived, Observed
PR-S2-A5-2	Number of protected alternates for a given mission-critical hardware component	Prepare	Maintain the resources needed to execute cyber courses of action: Maintain multiple protected instances of hardware	Diversity: Supply Chain Diversity; Redundancy: Replication	Maintain redundancy	EIT, LSPE, CPS	Engineering, Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured or Observed
PR-S2-A5-3	Degree of confidence in protection of alternate component (based on supply chain risk management (SCRM) controls)	Prepare	Maintain the resources needed to execute cyber courses of action: Maintain multiple protected instances of hardware	Diversity: Supply Chain Diversity; Redundancy: Replication	Maintain redundancy	EIT, LSPE, CPS	Engineering, Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged
PR-S2-A5-4	Percentage of hot vs cold/spare components for mission-critical hardware	Prepare	Maintain the resources needed to execute cyber courses of action: Maintain multiple protected instances of hardware	Diversity: Supply Chain Diversity; Redundancy: Replication	Maintain redundancy	EIT, LSPE, CPS	Engineering, Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Observed
PR-S2-A6-1	Percentage of key system elements for which architectural alternatives are maintained	Prepare	Maintain the resources needed to execute cyber courses of action: Acquire and maintain architectural alternatives for key system elements	Diversity: Architectural Diversity	Plan and manage diversity	EIT, LSPE, CPS	Engineering, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Observed
PR-S2-A6-2	Number of architectural alternatives for each type of key system element	Prepare	Maintain the resources needed to execute cyber courses of action: Acquire and maintain architectural alternatives for key system elements	Diversity: Architectural Diversity	Plan and manage diversity	EIT, LSPE, CPS	Engineering, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PR-S2-A7-1	Percentage of mission / business process threads for which alternative processing paths are available	Prepare	Maintain the resources needed to execute cyber courses of action: Define and maintain determinably different alternative processing paths	Diversity: Design Diversity	Plan and manage diversity	EIT, LSPE, CPS	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
PR-S2-A7-2	Time since last exercise of alternative processing paths for a given mission / business process thread	Prepare	Maintain the resources needed to execute cyber courses of action: Define and maintain determinably different alternative processing paths	Diversity: Design Diversity	Plan and manage diversity	EIT, LSPE, CPS	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Observed
PR-S2-A7-3	Frequency of alternate path usage	Prepare	Maintain the resources needed to execute cyber courses of action: Define and maintain determinably different alternative processing paths	Diversity: Design Diversity	Plan and manage diversity	EIT, LSPE, CPS	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived, Observed
PR-S2-A8-1	Percentage of communications paths for which alternatives are available	Prepare	Maintain the resources needed to execute cyber courses of action: Define and maintain determinably different alternative communications paths	Diversity: Path Diversity	Plan and manage diversity	EIT, LSPE, CPS	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived, Observed
PR-S2-A8-2	Time since last exercise of alternative communications paths	Prepare	Maintain the resources needed to execute cyber courses of action: Define and maintain determinably different alternative communications paths	Diversity: Path Diversity	Plan and manage diversity	EIT, LSPE, CPS	Engineering, Tactical Operations, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PR-S2-A9-1	Percentage of mission-critical Information / Technical components for which diverse supply chains are used	Prepare	Maintain the resources needed to execute cyber courses of action: Use determinably different supply chains for key Information / Technical components	Diversity: Supply Chain Diversity	Plan and manage diversity	EIT, LSPE, CPS, PIT	Engineering, Investment / Programmatic	Information / Technical, Social / Organizational	Judged, Observed
PR-S2-A9-2	Frequency of SCRM review	Prepare	Maintain the resources needed to execute cyber courses of action: Use determinably different supply chains for key Information / Technical components	Diversity: Supply Chain Diversity	Plan and manage diversity	EIT, LSPE, CPS, PIT	Engineering, Investment / Programmatic	Information / Technical, Social / Organizational	Judged, Observed
PR-S2-A9-3	Percentage of components with verified supply chain integrity	Prepare	Maintain the resources needed to execute cyber courses of action: Use determinably different supply chains for key Information / Technical components	Diversity: Supply Chain Diversity	Plan and manage diversity	EIT, LSPE, CPS, PIT	Engineering, Investment / Programmatic	Information / Technical, Social / Organizational	Computed or Derived, Observed
PR-S2-A10-1	Percentage of mission-critical data stores for which diverse data sources are available	Prepare	Maintain the resources needed to execute cyber courses of action: Identify and maintain determinably different mission data sources	Diversity: Information Diversity	Plan and manage diversity	EIT, LSPE, CPS	Engineering, Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Computed or Derived, Observed
PR-S2-A11-1	Percentage of mission-critical data types for which multiple different data stores are maintained	Prepare	Maintain the resources needed to execute cyber courses of action: Create and maintain determinably different information stores	Diversity: Information Diversity	Plan and manage diversity	EIT, LSPE, CPS	Engineering, Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Computed or Derived, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PR-S2-A11-2	Percentage of diverse datastores using unique technologies (e.g., SQL vs. noSQL)	Prepare	Maintain the resources needed to execute cyber courses of action: Create and maintain determinably different information stores	Diversity: Information Diversity	Plan and manage diversity	EIT, LSPE, CPS	Engineering, Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Computed or Derived, Observed
PR-S2-A12-1	Percentage of mission-critical data stores for which at least two gold copies (one current, one as-of a given prior date) are maintained	Prepare	Maintain the resources needed to execute cyber courses of action: Create and maintain multiple protected instances of information	Diversity: Information Diversity; Redundancy: Replication	Maintain redundancy	EIT, LSPE, CPS	Engineering, Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Computed or Derived, Observed
PR-S2-A12-2	Number and age of maintained gold copies	Prepare	Maintain the resources needed to execute cyber courses of action: Create and maintain multiple protected instances of information	Diversity: Information Diversity; Redundancy: Replication	Maintain redundancy	EIT, LSPE, CPS	Engineering, Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Observed
PR-S2-A13-1	Percentage of mission-critical software components for which a gold copy is maintained	Prepare	Maintain the resources needed to execute cyber courses of action: Create and maintain multiple protected instances of software	Diversity: Design Diversity, Synthetic Diversity; Redundancy: Replication	Maintain redundancy	EIT, LSPE, CPS	Engineering, Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Computed or Derived, Observed
PR-S2-A13-2	Percentage of mission-critical software components for which at least two gold copies (current, and previous) are maintained	Prepare	Maintain the resources needed to execute cyber courses of action: Create and maintain multiple protected instances of software	Diversity: Design Diversity, Synthetic Diversity; Redundancy: Replication	Maintain redundancy	EIT, LSPE, CPS	Engineering, Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Computed or Derived, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PR-S2-A13-3	Number and age of maintained gold copies	Prepare	Maintain the resources needed to execute cyber courses of action: Create and maintain multiple protected instances of software	Diversity: Design Diversity, Synthetic Diversity; Redundancy: Replication	Maintain redundancy	EIT, LSPE, CPS	Engineering, Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Observed
PR-S3-A1-1	Percentage of security controls or security administrative functions mapped to CCoAs which rely on those controls or functions	Prepare	Validate the realism of cyber courses of action: Validate expected dependencies and interactions among cyber defenses, security controls, and performance controls	Coordinated Protection: Consistency Analysis, Orchestration, Self-Challenge; Dynamic Representation: Dynamic Mapping and Profiling, Mission Dependency and Status Visualization	Determine ongoing trustworthiness, Maintain situational awareness	EIT, LSPE, CPS	Engineering, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged
PR-S3-A1-2	Percentage of performance controls or performance management functions mapped to CCoAs which rely on those controls or functions	Prepare	Validate the realism of cyber courses of action: Validate expected dependencies and interactions among cyber defenses, security controls, and performance controls	Coordinated Protection: Consistency Analysis, Orchestration, Self-Challenge; Dynamic Representation: Dynamic Mapping and Profiling, Mission Dependency and Status Visualization	Determine ongoing trustworthiness, Maintain situational awareness	EIT, LSPE, CPS	Engineering, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged
PR-S3-A2-1	Time since last [random, scheduled] exercise or simulation of one or more CCoAs	Prepare	Validate the realism of cyber courses of action: Simulate and/or exercise CCoAs	Coordinated Protection: Self-Challenge	Determine ongoing trustworthiness	EIT, LSPE, CPS	Engineering, COA Analysis	Cognitive (Cyber Operations), Social / Organizational	Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PR-S3-A2-2	Time since last [random, scheduled] exercise or simulation of all CCoAs in the organization's cyber playbook	Prepare, Continue	Validate the realism of cyber courses of action: Simulate and/or exercise CCoAs; Minimize interruptions in service delivery: Coordinate response activities to ensure synergy rather than interference	Coordinated Protection: Self-Challenge, Orchestration	Determine ongoing trustworthiness	EIT, LSPE, CPS	Engineering, COA Analysis	Cognitive (Cyber Operations), Social / Organizational	Observed
PR-S3-A2-3	Frequency of exercise	Prepare	Validate the realism of cyber courses of action: Simulate and/or exercise CCoAs	Coordinated Protection: Self-Challenge	Determine ongoing trustworthiness	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, COA Analysis	Cognitive (Cyber Operations), Social / Organizational	Observed
PR-S3-A2-4	Exercises performed on live system [yes/no]	Prepare	Validate the realism of cyber courses of action: Simulate and/or exercise CCoAs	Coordinated Protection: Self-Challenge	Determine ongoing trustworthiness	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, COA Analysis	Cognitive (Cyber Operations), Social / Organizational	Observed
PR-S3-A2-5	Exercises performed randomly [yes/no]	Prepare	Validate the realism of cyber courses of action: Simulate and/or exercise CCoAs	Coordinated Protection: Self-Challenge	Determine ongoing trustworthiness	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, COA Analysis	Cognitive (Cyber Operations), Social / Organizational	Observed
PR-S3-A2-6	Time since last exercise	Prepare	Validate the realism of cyber courses of action: Simulate and/or exercise CCoAs	Coordinated Protection: Self-Challenge	Determine ongoing trustworthiness	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, COA Analysis	Cognitive (Cyber Operations), Social / Organizational	Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
PR-S3-A2-7	Frequency of joint exercises	Prepare, Continue	Validate the realism of cyber courses of action: Simulate and/or exercise CCoAs; Minimize interruptions in service delivery: Coordinate response activities to ensure synergy rather than interference	Coordinated Protection: Self-Challenge, Orchestration	Determine ongoing trustworthiness	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, COA Analysis	Cognitive (Cyber Operations), Social / Organizational	Observed
CN-S1-A1-1	Percentage of mission-critical data assets for which data integrity / quality has been validated since initiation of CCoA	Continue	Minimize degradation of service delivery: Perform mission damage assessment; Minimize interruptions in service delivery: Perform mission damage assessment; Ensure that ongoing functioning is correct: Validate data integrity / quality to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks	Determine ongoing trustworthiness	EIT, Federated EIT, LSPE, CPS, Federated CPS	Engineering, Tactical Operations, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Measured, Observed, Computed or Derived
CN-S1-A2-2	Percentage of mission-critical applications for which integrity / behavior has been validated since initiation of CCoA	Continue	Ensure that ongoing functioning is correct: Validate software / service integrity / behavior to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks, Behavior Validation	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
CN-S1-A1-3	Percentage of security-critical applications for which integrity / behavior has been validated since initiation of CCoA	Continue	Minimize degradation of service delivery: Perform damage assessment; Minimize interruption of service delivery: Perform damage assessment; Ensure that ongoing functioning is correct: Validate software / service integrity / behavior to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks, Behavior Validation	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CN-S1-A2-1	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]	Continue	Minimize degradation of service delivery: Maintain acceptable levels of performance for mission-critical, security-critical, and mission-supporting applications and services	Adaptive Response: Adaptive Management; Dynamic Representation: Mission Dependency and Status Visualization	Manage resources (risk-) adaptively	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured or Observed
CN-S1-A2-2	Percentage of security-critical applications and services for which MOPs remain at or above their required levels over (specified) time period	Continue	Minimize degradation of service delivery: Maintain acceptable levels of performance for mission-critical, security-critical, and mission-supporting applications and services	Adaptive Response: Adaptive Management; Dynamic Representation: Mission Dependency and Status Visualization	Manage resources (risk-) adaptively	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured or Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
CN-S1-A2-3	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]	Continue	Minimize degradation of service delivery: Maintain acceptable levels of performance for mission-critical, security-critical, and mission-supporting applications and services	Adaptive Response: Adaptive Management; Dynamic Representation: Mission Dependency and Status Visualization	Manage resources (risk-) adaptively	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured or Observed
CN-S1-A3-1	Time between selection of CCoA and completion of tailoring	Continue	Minimize degradation of service delivery: Select and tailor CCoA	Adaptive Response: Adaptive Management; Dynamic Representation: Mission Dependency and Status Visualization	Manage resources (risk-) adaptively	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Measured, Observed
CN-S1-A3-2	Time between determination that a CCoA must be taken and initiation of tailored CCoA	Continue	Minimize degradation of service delivery: Select and tailor CCoA	Adaptive Response: Adaptive Management; Dynamic Representation: Mission Dependency and Status Visualization	Manage resources (risk-) adaptively	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Measured, Observed
CN-S1-A4-1	Percentage of cyber resources which can be reconfigured on demand	Continue	Minimize degradation of service delivery: Dynamically reconfigure existing resources	Adaptive Response: Dynamic Reconfiguration	Manage resources (risk-) adaptively	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged
CN-S1-A4-2	Time between decision to reconfigure resources and completion of reconfiguration	Continue	Minimize degradation of service delivery: Dynamically reconfigure existing resources	Adaptive Response: Dynamic Reconfiguration	Manage resources (risk-) adaptively	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Measured, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
CN-S1-A4-3	Percentage of cyber resources which can be [automatically, manually] reconfigured	Continue	Minimize degradation of service delivery: Dynamically reconfigure existing resources	Adaptive Response: Dynamic Reconfiguration	Manage resources (risk-) adaptively	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Observed
CN-S1-A5-1	Percentage of cyber resources which can be reallocated on demand	Continue	Minimize degradation of service delivery: Dynamically provision by reallocating existing resources	Adaptive Response: Dynamic Reallocation; Redundancy: Surplus Capacity	Manage resources (risk-) adaptively	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Observed
CN-S1-A5-2	Time between decision to reallocate resources and completion of reallocation	Continue	Minimize degradation of service delivery: Dynamically provision by reallocating existing resources	Adaptive Response: Dynamic Reallocation; Redundancy: Surplus Capacity	Manage resources (risk-) adaptively	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Measured, Observed
CN-S1-A6-1	Percentage of critical capabilities which can be recreated by combining existing resources in a novel way	Continue	Minimize degradation of service delivery: Dynamically recreate critical capabilities by combining existing resources in a novel way	Adaptive Response: Dynamic Reconfiguration	Manage resources (risk-) adaptively	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Observed
CN-S1-A6-2	Time between decision to recreate resources and completion of the process	Continue	Minimize degradation of service delivery: Dynamically recreate critical capabilities by combining existing resources in a novel way	Adaptive Response: Dynamic Reconfiguration	Manage resources (risk-) adaptively	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Observed
CN-S1-A7-1	Time between decision to relocate resources and completion of relocation	Continue	Minimize degradation of service delivery: Relocate resources to minimize service degradation	Adaptive Response: Adaptive Management; Dynamic Positioning: Asset Mobility, Functional Relocation of Cyber Resources	Manage resources (risk-) adaptively	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Observed
CN-S1-A7-2	Frequency with which relocation occurs	Continue	Minimize degradation of service delivery: Relocate resources to minimize service degradation	Adaptive Response: Adaptive Management; Dynamic Positioning: Asset Mobility, Functional Relocation of Cyber Resources	Manage resources (risk-) adaptively	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
CN-S2-A2-1	Time between selection of CCoA and completion of tailoring	Continue	Minimize interruptions in service delivery: Select and tailor CCoA	Adaptive Response: Adaptive Management; Dynamic Representation: Mission Dependency and Status Visualization	Manage resources (risk-) adaptively	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Measured, Observed, Computed or Derived
CN-S2-A2-2	Time between determination that a CCoA must be taken and initiation of tailored CCoA	Continue	Minimize interruptions in service delivery: Select and tailor CCoA	Adaptive Response: Adaptive Management; Dynamic Representation: Mission Dependency and Status Visualization	Manage resources (risk-) adaptively	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Measured, Observed, Computed or Derived
CN-S2-A3-1	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	Continue	Minimize interruptions in service delivery: Coordinate response activities to ensure synergy rather than interference	Coordinated Protection: Orchestration	Manage resources (risk-) adaptively	EIT, Federated EIT, LSPE, CPS, Federated CPS	COA Analysis	Social / Organizational	Judged
CN-S2-A4-1	Time between decision to redeploy resources and completion of redeployment	Continue	Minimize interruptions in service delivery: Deploy diverse resources rapidly (e.g., in near real time)	Adaptive Response: Dynamic Reconfiguration, Diversity: Architectural Diversity, Design Diversity, Synthetic Diversity, Path Diversity	Manage resources (risk-) adaptively, Plan and manage diversity	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Measured, Observed, Computed or Derived
CN-S2-A4-2	Number of differences between initial set of resources and redeployed set	Continue	Minimize interruptions in service delivery: Deploy diverse resources rapidly (e.g., in near real time)	Adaptive Response: Dynamic Reconfiguration, Diversity: Architectural Diversity, Design Diversity, Synthetic Diversity, Path Diversity	Manage resources (risk-) adaptively, Plan and manage diversity	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
CN-S2-A5-1	Average, median, or maximum time to fail over mission-critical functions over [specify period over which measurements are taken]	Continue	Minimize interruptions in service delivery: Fail over to replicated resources	Adaptive Response: Dynamic Reconfiguration; Redundancy: Protected Backup and Restore, Replication	Manage resources (risk-) adaptively, Maintain redundancy	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CN-S2-A5-2	Percentage of failovers which met required MOPs during [specify period over which measurements are taken]	Continue	Minimize interruptions in service delivery: Fail over to replicated resources	Adaptive Response: Dynamic Reconfiguration; Redundancy: Protected Backup and Restore, Replication	Manage resources (risk-) adaptively, Maintain redundancy	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CN-S2-A5-3	Time since last test of failover	Continue	Minimize interruptions in service delivery: Fail over to replicated resources	Adaptive Response: Dynamic Reconfiguration; Redundancy: Protected Backup and Restore, Replication	Manage resources (risk-) adaptively, Maintain redundancy	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CN-S2-A6-1	Time to replace a mission-critical hardware component with a protected alternate	Continue	Minimize interruptions in service delivery: Replace suspect hardware components with protected alternates	Adaptive Response: Dynamic Reconfiguration; Diversity: Supply Chain Diversity; Redundancy: Replication	Manage resources (risk-) adaptively, Maintain redundancy	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CN-S2-A6-2	Confidence that alternate is not affected by similar issues	Continue	Minimize interruptions in service delivery: Replace suspect hardware components with protected alternates	Adaptive Response: Dynamic Reconfiguration; Diversity: Supply Chain Diversity; Redundancy: Replication	Manage resources (risk-) adaptively, Maintain redundancy	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged
CN-S2-A7-1	Average, median, or maximum time to switch a mission-critical function to an alternative processing path	Continue	Minimize interruptions in service delivery: Switch processing to use alternative processing paths	Adaptive Response: Dynamic Reconfiguration; Diversity: Design Diversity	Manage resources (risk-) adaptively, Plan and manage diversity	EIT, Federated EIT, LSPE, CPS, Federated CPS	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
CN-S2-A7-2	Frequency of use/test of alternative processing paths	Continue	Minimize interruptions in service delivery: Switch processing to use alternative processing paths	Adaptive Response: Dynamic Reconfiguration; Diversity: Design Diversity	Manage resources (risk-) adaptively, Plan and manage diversity	EIT, Federated EIT, LSPE, CPS, Federated CPS	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Measured, Observed
CN-S2-A8-1	Average, median, or maximum time to switch a mission-critical connection to an alternative communications path	Continue	Minimize interruptions in service delivery: Switch communications to use alternative communications paths	Adaptive Response: Dynamic Reconfiguration; Diversity: Path Diversity	Manage resources (risk-) adaptively, Plan and manage diversity	EIT, Federated EIT, LSPE, CPS, Federated CPS	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CN-S2-A8-2	Frequency of use/test of alternative communications paths	Continue	Minimize interruptions in service delivery: Switch communications to use alternative communications paths	Adaptive Response: Dynamic Reconfiguration; Diversity: Path Diversity	Manage resources (risk-) adaptively, Plan and manage diversity	EIT, Federated EIT, LSPE, CPS, Federated CPS	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Measured, Observed
CN-S2-A9-1	Average, median, or maximum time to locate and switch over to an alternative mission data source	Continue	Minimize interruptions in service delivery: Locate and switch over to alternative mission data sources	Adaptive Response: Dynamic Reconfiguration; Diversity: Information Diversity	Manage resources (risk-) adaptively, Plan and manage diversity	EIT, Federated EIT, LSPE, CPS, Federated CPS	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CN-S2-A10-1	Average, median, or maximum time to locate and switch over to an alternative information store	Continue	Minimize interruptions in service delivery: Locate and switch over to alternative information stores	Adaptive Response: Dynamic Reconfiguration; Diversity: Information Diversity	Manage resources (risk-) adaptively, Plan and manage diversity	EIT, Federated EIT, LSPE, CPS, Federated CPS	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CN-S3-A1-1	Percentage of mission-critical and system control data for which provenance has been validated since the initiation of the CCoA	Continue	Ensure that ongoing functioning is correct: Validate provenance of mission-critical and system control data	Substantiated Integrity: Provenance Tracking	Determine ongoing trustworthiness	EIT, Federated EIT, LSPE, CPS, Federated CPS	Engineering, Tactical Operations, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
CN-S3-A1-2	Percentage of security-critical data for which provenance has been validated since the initiation of the CCoA	Continue	Ensure that ongoing functioning is correct: Validate provenance of mission-critical and system control data	Substantiated Integrity: Provenance Tracking	Determine ongoing trustworthiness	EIT, Federated EIT, LSPE, CPS, Federated CPS	Engineering, Tactical Operations, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CN-S3-A3-2	Percentage of mission-critical applications for which integrity / behavior has been validated since initiation of CCoA	Continue	Ensure that ongoing functioning is correct: Validate software / service integrity / behavior to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks, Behavior Validation	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CN-S3-A3-4	Percentage of security-critical applications for which integrity / behavior has been validated since initiation of CCoA	Continue	Ensure that ongoing functioning is correct: Validate software / service integrity / behavior to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks, Behavior Validation	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CN-S3-A4-1	Percentage of mission-critical systems or system elements for which integrity / behavior has been validated since initiation of CCoA	Continue	Ensure that ongoing functioning is correct: Validate hardware / system integrity / behavior to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks, Behavior Validation	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CN-S3-A4-2	Percentage of security-critical systems or system elements for which integrity / behavior has been validated since initiation of CCoA	Continue	Ensure that ongoing functioning is correct: Validate hardware / system integrity / behavior to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks, Behavior Validation	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
CS-S1-A1-1	Time between detection or notification of a triggering event and completion of the identification / assessment process	Constrain	Identify potential damage: Identify potentially corrupted or falsified information	Analytic Monitoring: Monitoring and Damage Assessment; Substantiated Integrity: Integrity Checks	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CS-S1-A1-2	Number of locations where corrupted / falsified information checks occur	Constrain	Identify potential damage: Identify potentially corrupted or falsified information	Analytic Monitoring: Monitoring and Damage Assessment; Substantiated Integrity: Integrity Checks	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed
CS-S1-A2-1	Percentage of mission-critical applications for which integrity / behavior is validated	Constrain	Identify potential damage: Identify potentially compromised or faulty processes or services	Analytic Monitoring: Monitoring and Damage Assessment; Substantiated Integrity: Behavior Validation	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CS-S1-A2-2	Percentage of mission-supporting applications for which integrity / behavior is validated	Constrain	Identify potential damage: Identify potentially compromised or faulty processes or services	Analytic Monitoring: Monitoring and Damage Assessment; Substantiated Integrity: Behavior Validation	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Computed or Derived
CS-S1-A2-3	Time between detection or notification of a triggering event and completion of the identification / assessment process	Constrain	Identify potential damage: Identify potentially compromised or faulty processes or services	Analytic Monitoring: Monitoring and Damage Assessment; Substantiated Integrity: Behavior Validation	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Computed or Derived
CS-S1-A3-1	Percentage of components to which anti-tampering has been applied which are checked in the operational environment	Constrain	Identify potential damage: Identify potentially faulty, corrupted, or subverted components	Substantiated Integrity: Integrity Checks	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
CS-S1-A3-2	Frequency of checking for tamper-evidence	Constrain	Identify potential damage: Identify potentially faulty, corrupted, or subverted components	Substantiated Integrity: Integrity Checks	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CS-S1-A3-3	Elapsed time between detection or notification of a triggering event and completion of the process of checking for tamper evidence	Constrain	Identify potential damage: Identify potentially faulty, corrupted, or subverted components	Substantiated Integrity: Integrity Checks	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CS-S2-A1-1	Time between decision to isolate an enclave or a set of cyber resources and completion of isolation	Constrain	Isolate resources to limit future or further damage: Isolate a suspicious enclave or set of cyber resources, Isolate a critical or sensitive enclave or set of cyber resources	Adaptive Response: Adaptive Management; Segmentation: Dynamic Segmentation and Isolation	Manage resources (risk-) adaptively, Contain and exclude behaviors	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed
CS-S2-A1-2	Percentage or number of dynamically isolated cyber resources which can be discovered, accessed or used, or otherwise reached from some point in the network	Constrain	Isolate resources to limit future or further damage: Isolate a suspicious enclave or set of cyber resources, Isolate a critical or sensitive enclave or set of cyber resources	Adaptive Response: Adaptive Management; Segmentation: Dynamic Segmentation and Isolation	Manage resources (risk-) adaptively, Contain and exclude behaviors	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed
CS-S2-A1-3	Percentage or number of resources outside an isolated enclave compromised post isolation	Constrain	Isolate resources to limit future or further damage: Isolate a suspicious enclave or set of cyber resources, Isolate a critical or sensitive enclave or set of cyber resources	Adaptive Response: Adaptive Management; Segmentation: Dynamic Segmentation and Isolation	Manage resources (risk-) adaptively, Contain and exclude behaviors	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
CS-S3-A2-1	Percentage of critical assets which can be physically relocated (i.e., to another facility)	Constrain	Move resources to limit future or further damage: Dynamically relocate critical resources	Dynamic Positioning: Asset Mobility, Functional Relocation of Cyber Resources	Make resources location-versatile	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed
CS-S3-A2-2	Percentage of critical assets which can be logically relocated (e.g., to a different VM)	Constrain	Move resources to limit future or further damage: Dynamically relocate critical resources	Dynamic Positioning: Asset Mobility, Functional Relocation of Cyber Resources	Make resources location-versatile	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed
CS-S3-A2-3	Time between decision to relocate a critical asset and the initial use of the relocated asset	Constrain	Move resources to limit future or further damage: Dynamically relocate critical resources	Dynamic Positioning: Asset Mobility, Functional Relocation of Cyber Resources	Make resources location-versatile	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CS-S3-A3-1	Percentage of non-critical assets which have been analyzed with respect to the exposure they present to critical assets if compromised	Constrain	Move resources to limit future or further damage: 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	Make resources location-versatile	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged
CS-S3-A3-2	Percentage of non-critical assets which have been reassigned or relocated to reduce the exposure they offer to critical assets if compromised	Constrain	Move resources to limit future or further damage: 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	Make resources location-versatile	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CS-S3-A3-3	Time between decision to reassign or relocate a resource and the initial use of the relocated resource	Constrain	Move resources to limit future or further damage: 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	Make resources location-versatile	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
CS-S4-A1-1	Time between determination to recreate an application or service and discovery of resources from which it can be recreated	Constrain	Change or remove resources and how they are used to limit future or further damage: Recreate applications or services	Adaptive Response: Adaptive Management; Diversity: Synthetic Diversity; Non-Persistence: Non-Persistent Services	Manage resources (risk-) adaptively, Make resources location-versatile	EIT, LSPE	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CS-S4-A1-2	Time between determination to recreate an application or service and the new instance becoming active or operational	Constrain	Change or remove resources and how they are used to limit future or further damage: Recreate applications or services	Adaptive Response: Adaptive Management; Diversity: Synthetic Diversity; Non-Persistence: Non-Persistent Services	Manage resources (risk-) adaptively, Make resources location-versatile	EIT, LSPE	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CS-S4-A1-3	Time between determination to recreate an application or service and the new instance being used by other system elements	Constrain	Change or remove resources and how they are used to limit future or further damage: Recreate applications or services	Adaptive Response: Adaptive Management; Diversity: Synthetic Diversity; Non-Persistence: Non-Persistent Services	Manage resources (risk-) adaptively, Make resources location-versatile	EIT, LSPE	Engineering, Tactical Operations, COA Analysis	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CS-S4-A4-1	Percentage of resources which are relocated virtually randomly or as part of a CCoA	Constrain	Change or remove resources and how they are used to limit future or further damage: Dynamically relocate processing	Adaptive Response: Dynamic Reconfiguration; Dynamic Positioning: Asset Mobility, Functional Relocation of Cyber Resources; Unpredictability	Manage resources (risk-) adaptively, Make resources location-versatile	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
CS-S4-A4-2	Percentage of resources which are relocated physically randomly or as part of a CCoA	Constrain	Change or remove resources and how they are used to limit future or further damage: Dynamically relocate processing	Adaptive Response: Dynamic Reconfiguration; Dynamic Positioning: Asset Mobility, Functional Relocation of Cyber Resources; Unpredictability	Manage resources (risk-) adaptively, Make resources location-versatile	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CS-S4-A4-3	Average time to complete the relocation process (latency or lag)	Constrain	Change or remove resources and how they are used to limit future or further damage: Dynamically relocate processing	Adaptive Response: Dynamic Reconfiguration; Dynamic Positioning: Asset Mobility, Functional Relocation of Cyber Resources; Unpredictability	Manage resources (risk-) adaptively, Make resources location-versatile	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CS-S4-A4-4	Frequency of relocation events per unit time	Constrain	Change or remove resources and how they are used to limit future or further damage: Dynamically relocate processing	Adaptive Response: Dynamic Reconfiguration; Dynamic Positioning: Asset Mobility, Functional Relocation of Cyber Resources; Unpredictability	Manage resources (risk-) adaptively, Make resources location-versatile	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CS-S4-A7-1	Percentage of cyber resources for which privileges are modified randomly or as part of a CCoA	Constrain	Change or remove resources and how they are used to limit future or further damage: Modify privilege restrictions	Privilege Restriction: Dynamic Privileges; Unpredictability: Temporal Unpredictability, Contextual Unpredictability	Manage resources (risk-) adaptively	EIT, LSPE	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
CS-S4-A7-2	Percentage of users for whom privileges can be modified dynamically whose privileges are modified randomly or as part of a CCoA	Constrain	Change or remove resources and how they are used to limit future or further damage: Modify privilege restrictions	Privilege Restriction: Dynamic Privileges; Unpredictability: Temporal Unpredictability, Contextual Unpredictability	Manage resources (risk-) adaptively	EIT, LSPE	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
CS-S4-A7-3	Percentage of system services for which privileges can be modified dynamically for which privileges are modified randomly or as part of a CCoA	Constrain	Change or remove resources and how they are used to limit future or further damage: Modify privilege restrictions	Privilege Restriction: Dynamic Privileges; Unpredictability: Temporal Unpredictability, Contextual Unpredictability	Manage resources (risk-) adaptively	EIT, LSPE	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S1-A1-1	Time to identify unavailable resources and represent damage in status visualization	Reconstitute	Identify damage and untrustworthy resources: Identify lost resources	Analytic Monitoring: Monitoring and Damage Assessment; Dynamic Representation: Mission Dependency and Status Visualization	Leverage health and status data	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S1-A1-2	Time to notify services or mission / business functions which use damaged or unavailable resources that those resources are no longer available	Reconstitute	Identify damage and untrustworthy resources: Identify lost resources	Analytic Monitoring: Monitoring and Damage Assessment; Dynamic Representation: Mission Dependency and Status Visualization	Leverage health and status data	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S1-A2-1	Time to identify suspect [mission-critical, security-critical, supporting] information	Reconstitute	Identify damage and untrustworthy resources: Identify corrupted, falsified, or suspect information	Analytic Monitoring: Monitoring and Damage Assessment; Substantiated Integrity: Integrity Checks	Leverage health and status data	EIT, LSPE, CPS, PIT	Tactical Operations	Cognitive (Cyber Operations)	
RE-S1-A2-2	Time to notify services or mission / business functions which use suspect information to delete or disregard that information	Reconstitute	Identify damage and untrustworthy resources: Identify corrupted, falsified, or suspect information	Analytic Monitoring: Monitoring and Damage Assessment; Substantiated Integrity: Integrity Checks	Leverage health and status data	EIT, LSPE, CPS, PIT	Tactical Operations	Cognitive (Cyber Operations)	Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
RE-S1-A3-1	Percentage of [mission-critical, security-critical, supporting] processes or services which are validated	Reconstitute	Identify damage and untrustworthy resources: 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	Leverage health and status data	EIT, LSPE, CPS, PIT	Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S1-A3-2	Time to identify suspect [mission-critical, security-critical, supporting] processes or services	Reconstitute	Identify damage and untrustworthy resources: 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	Leverage health and status data	EIT, LSPE, CPS, PIT	Tactical Operations	Cognitive (Cyber Operations)	Measured, Observed, Computed or Derived
RE-S1-A3-3	Time to notify services or mission / business functions which use or communicate with suspect processes or services to terminate interactions with those services	Reconstitute	Identify damage and untrustworthy resources: 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	Leverage health and status data	EIT, LSPE, CPS, PIT	Tactical Operations	Cognitive (Cyber Operations)	Measured, Observed, Computed or Derived
RE-S1-A4-1	Percentage of mission critical components that employ anti-tamper, shielding, and power line filtering which are checked	Reconstitute	Identify damage and untrustworthy resources: Identify damaged, corrupted, or subverted components	Substantiated Integrity: Integrity Checks	Leverage health and status data	EIT, LSPE, CPS, PIT	Engineering, Investment / Programmatic	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S1-A4-2	Time to identify damaged components	Reconstitute	Identify damage and untrustworthy resources: Identify damaged, corrupted, or subverted components	Substantiated Integrity: Integrity Checks	Leverage health and status data	EIT, LSPE, CPS, PIT	Engineering, Investment / Programmatic	Cognitive (Cyber Operations)	Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
RE-S2-A1-1	Percentage of mission capabilities for which [minimum acceptable, target] MOPs are achieved within [minimum threshold, target] period of time since initiating event	Reconstitute	Restore functionality: Execute recovery procedures in accordance with contingency or continuity of operations plans	Coordinated Protection: Orchestration; Redundancy: Protected Backup and Restore	Maintain redundancy	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S2-A1-2	Percentage of mission-critical cyber resources which are recovered from a backup	Reconstitute	Restore functionality: Execute recovery procedures in accordance with contingency or continuity of operations plans	Coordinated Protection: Orchestration; Redundancy: Protected Backup and Restore	Maintain redundancy	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S2-A1-3	Size of gap between lost and recovered mission-critical resources (time service or connection was unavailable, number of records not recovered)	Reconstitute	Restore functionality: Execute recovery procedures in accordance with contingency or continuity of operations plans	Coordinated Protection: Orchestration; Redundancy: Protected Backup and Restore	Maintain redundancy	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S2-A2-1	Time between event or detected circumstances which motivated recovery procedures and achievement of [minimum acceptable, target] MOPs for supporting functional capabilities	Reconstitute	Restore functionality: Restore non-critical functional capabilities	Adaptive Response: Dynamic Reconfiguration, Dynamic Resource Allocation; Redundancy: Protected Backup and Restore	Manage resources (risk-) adaptively, Maintain redundancy	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
RE-S2-A2-2	Percentage of supporting functional capabilities for which [minimum acceptable, target] MOPs are achieved within [minimum threshold, target] period of time since initiating event	Reconstitute	Restore functionality: Restore non-critical functional capabilities	Adaptive Response: Dynamic Reconfiguration, Dynamic Resource Allocation; Redundancy: Protected Backup and Restore	Manage resources (risk-) adaptively, Maintain redundancy	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S2-A2-3	Percentage of non-mission-critical resources which are recovered from a backup	Reconstitute	Restore functionality: Restore non-critical functional capabilities	Adaptive Response: Dynamic Reconfiguration, Dynamic Resource Allocation; Redundancy: Protected Backup and Restore	Manage resources (risk-) adaptively, Maintain redundancy	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S2-A2-4	Size of gap between lost and recovered non-mission-critical resources (time service or connection was unavailable, number of records not recovered)	Reconstitute	Restore functionality: Restore non-critical functional capabilities	Adaptive Response: Dynamic Reconfiguration, Dynamic Resource Allocation; Redundancy: Protected Backup and Restore	Manage resources (risk-) adaptively, Maintain redundancy	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S2-A3-1	Percentage of cyber resources for which access control is maintained throughout the recovery process	Reconstitute	Restore functionality: Coordinate recovery activities to avoid gaps in security coverage	Adaptive Response: Adaptive Management; Privilege Restriction: Attribute-Based Usage Restrictions	Manage resources (risk-) adaptively, Maintain redundancy	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
RE-S2-A3-2	Percentage of cyber resources for which access controls at multiple levels or using different mechanisms are maintained consistently throughout the recovery process	Reconstitute	Restore functionality: Coordinate recovery activities to avoid gaps in security coverage	Adaptive Response: Adaptive Management; Coordinated Protection: Orchestration, Calibrated Defense-in-Depth; Privilege Restriction: Attribute-Based Usage Restrictions	Manage resources (risk-) adaptively, Maintain redundancy	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S2-A3-3	Percentage of cyber resources for which auditing or monitoring is maintained throughout the recovery process	Reconstitute	Restore functionality: Coordinate recovery activities to avoid gaps in security coverage	Adaptive Response: Adaptive Management; Analytic Monitoring: Monitoring and Damage Assessment; Dynamic Positioning: Functional Relocation of Sensors; Dynamic Representation: Mission Dependency and Status Visualization	Manage resources (risk-) adaptively, Maintain redundancy	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S2-A3-4	Duration of gap in auditing or monitoring for [mission-critical resource, non-mission-critical resource] during recovery	Reconstitute	Restore functionality: Coordinate recovery activities to avoid gaps in security coverage	Adaptive Response: Adaptive Management; Analytic Monitoring: Monitoring and Damage Assessment; Dynamic Positioning: Functional Relocation of Sensors; Dynamic Representation: Mission Dependency and Status Visualization		EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S2-A4-1	Percentage of compromised critical information stores which are reconstructed from existing resources	Reconstitute	Restore functionality: Reconstruct compromised critical assets or capabilities from existing resources	Adaptive Response: Dynamic Reconfiguration; Coordinated Protection: Orchestration; Dynamic Positioning: Fragmentation		EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
RE-S2-A4-2	Percentage of compromised critical information stores which are irretrievably lost	Reconstitute	Restore functionality: Reconstruct compromised critical assets or capabilities from existing resources	Adaptive Response: Dynamic Reconfiguration; Coordinated Protection: Orchestration; Dynamic Positioning: Fragmentation	Manage resources (risk-) adaptively, Maintain redundancy	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S2-A4-3	Percentage of compromised services or functions which are reconstructed from existing resources	Reconstitute	Restore functionality: Reconstruct compromised critical assets or capabilities from existing resources	Adaptive Response: Dynamic Reconfiguration; Coordinated Protection: Orchestration; Dynamic Positioning: Distributed Functionality	Manage resources (risk-) adaptively, Maintain redundancy	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S2-A4-4	Time to reconstruct an asset or capability from existing resources	Reconstitute	Restore functionality: Reconstruct compromised critical assets or capabilities from existing resources	Adaptive Response: Dynamic Reconfiguration; Coordinated Protection: Orchestration; Dynamic Positioning: Fragmentation, Distributed Functionality	Manage resources (risk-) adaptively, Maintain redundancy	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Measured, Observed, Computed or Derived
RE-S2-A4-5	Time to reconstruct an asset or capability from the current gold image	Reconstitute	Restore functionality: Reconstruct compromised critical assets or capabilities from existing resources	Adaptive Response: Dynamic Reconfiguration; Coordinated Protection: Orchestration; Dynamic Positioning: Fragmentation, Distributed Functionality	Manage resources (risk-) adaptively, Maintain redundancy	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
RE-S2-A4-6	Time to reconstruct an asset or capability from a previous gold image	Reconstitute	Restore functionality: Reconstruct compromised critical assets or capabilities from existing resources	Adaptive Response: Dynamic Reconfiguration; Coordinated Protection: Orchestration; Dynamic Positioning: Fragmentation, Distributed Functionality	Manage resources (risk-) adaptively, Maintain redundancy	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Measured, Observed, Computed or Derived
RE-S2-A4-7	Minimum amount of information or service loss necessary to make the system inoperable	Reconstitute	Restore functionality: Reconstruct compromised critical assets or capabilities from existing resources	Adaptive Response: Dynamic Reconfiguration; Coordinated Protection: Orchestration; Dynamic Positioning: Fragmentation, Distributed Functionality	Manage resources (risk-) adaptively, Maintain redundancy	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S3-A1-1	Percentage of cyber resources for which additional auditing or monitoring is applied during and after the recovery process	Reconstitute	Heighten protections during reconstitution: Intensify monitoring of restored or reconstructed resources	Adaptive Response: Adaptive Management; Dynamic Positioning: Functional Relocation of Sensors	Manage resources (risk-) adaptively, Maintain redundancy	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S3-A2-1	Percentage of reconstituted cyber resources for which more stringent access controls are applied during and after reconstitution	Reconstitute	Heighten protections during reconstitution: 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	Contain and exclude behaviors, Maintain redundancy	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
RE-S3-A2-2	Percentage of reconstituted cyber resources which are placed in a restricted enclave for a period after reconstitution	Reconstitute	Heighten protections during reconstitution: 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	Contain and exclude behaviors, Maintain redundancy	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S4-A1	Percentage of restored or reconstructed [mission-critical, security-critical, supporting] data assets for which data provenance is validated	Reconstitute	Determine the trustworthiness of restored or reconstructed resources: Validate data provenance of restored or reconstructed resources	Substantiated Integrity: Provenance Tracking	Maintain redundancy, Leverage health and status data	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
RE-S4-A2-1	Percentage of restored or reconstructed [mission-critical, security-critical, supporting] data assets for which data integrity / quality is checked	Reconstitute	Determine the trustworthiness of restored or reconstructed resources: Validate data integrity / quality of restored or reconstructed resources to ensure they not been corrupted	Substantiated Integrity: Integrity Checks	Maintain redundancy, Leverage health and status data	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
RE-S4-A3-1	Percentage of restored or reconstructed [mission-critical, security-critical, supporting] applications, services, and processes for which behavior is checked	Reconstitute	Determine the trustworthiness of restored or reconstructed resources: Validate software / service integrity / behavior of restored or reconstructed applications, services, and processes to ensure they have not been corrupted	Substantiated Integrity: Behavior Validation	Maintain redundancy, Leverage health and status data	EIT, LSPE, CPS, PIT	Engineering, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed, Computed or Derived
UN-S1-A1-1	Number of threat information feeds the organization uses	Understand	Understand adversaries: Use shared threat information	Analytic Monitoring: Sensor Fusion and Analysis; Dynamic Representation: Dynamic Threat Modeling	Maintain situational awareness	EIT, LSPE, CPS, PIT	COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations), Social / Organizational	Judged, Observed
UN-S1-A1-2	Frequency with which receipt of threat information is updated	Understand	Understand adversaries: Use shared threat information	Analytic Monitoring: Sensor Fusion and Analysis; Dynamic Representation: Dynamic Threat Modeling	Maintain situational awareness	EIT, LSPE, CPS, PIT	COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations), Social / Organizational	Judged, Observed
UN-S1-A1-3	Time between receipt of threat intelligence and determination of its relevance	Understand	Understand adversaries: Use shared threat information	Analytic Monitoring: Sensor Fusion and Analysis; Dynamic Representation: Dynamic Threat Modeling	Maintain situational awareness	EIT, LSPE, CPS, PIT	COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations), Social / Organizational	Judged, Observed
UN-S1-A1-4	Time between determination that threat intelligence is relevant and promulgation of defensive TTPs	Understand	Understand adversaries: Use shared threat information	Analytic Monitoring: Sensor Fusion and Analysis; Dynamic Representation: Dynamic Threat Modeling	Maintain situational awareness	EIT, LSPE, CPS, PIT	COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations), Social / Organizational	Judged, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
UN-S1-A1-5	Frequency with which the organization provides threat information to the broader community	Understand	Understand adversaries: Use shared threat information	Analytic Monitoring: Sensor Fusion and Analysis; Dynamic Representation: Dynamic Threat Modeling	Maintain situational awareness	EIT, LSPE, CPS, PIT	COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations), Social / Organizational	Judged, Observed
UN-S1-A1-6	Number of threat types/communities the organization monitors	Understand	Understand adversaries: Use shared threat information	Analytic Monitoring: Sensor Fusion and Analysis; Dynamic Representation: Dynamic Threat Modeling	Maintain situational awareness	EIT, LSPE, CPS, PIT	COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations), Social / Organizational	Judged, Observed
UN-S1-A2-1	Time between initiation of malware or forensic analysis and use or sharing of results of analysis	Understand	Understand adversaries: Reveal adversary TTPs by analysis	Analytic Monitoring: Malware and Forensic Analysis	Maintain situational awareness	EIT, LSPE, CPS, PIT	COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations)	Judged, Observed
UN-S1-A2-2	Average number per campaign or intrusion set of indicators or observables developed by self-analysis of malware or other artifacts	Understand	Understand adversaries: Reveal adversary TTPs by analysis	Analytic Monitoring: Malware and Forensic Analysis	Maintain situational awareness	EIT, LSPE, CPS	COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations)	Judged, Observed
UN-S1-A3-1	Number of deception environments provided	Understand	Understand adversaries: Observe and analyze adversary activities in deception environments	Deception: Misdirection; Analytic Monitoring: Sensor Fusion and Analysis; Dynamic Representation: Dynamic Threat Modeling	Make the effects of deception and unpredictability user-transparent, Maintain situational awareness	EIT, LSPE, CPS	COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations)	Judged, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
UN-S1-A3-2	Representativeness of deception environment – size [ratio of number of cyber resources in deception enclave to number of cyber resources in real enclave]	Understand	Understand adversaries: Observe and analyze adversary activities in deception environments	Deception: Misdirection; Analytic Monitoring: Sensor Fusion and Analysis; Dynamic Representation: Dynamic Threat Modeling	Make the effects of deception and unpredictability user-transparent, Maintain situational awareness	EIT, LSPE, CPS	COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations)	Judged, Observed
UN-S1-A3-3	Percentage of enclaves providing deception	Understand	Understand adversaries: Observe and analyze adversary activities in deception environments	Deception: Misdirection; Analytic Monitoring: Sensor Fusion and Analysis; Dynamic Representation: Dynamic Threat Modeling	Make the effects of deception and unpredictability user-transparent, Maintain situational awareness	EIT, LSPE, CPS	COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations)	Judged, Observed
UN-S1-A3-4	Number of observables or indicators developed per adversary engagement	Understand	Understand adversaries: Observe and analyze adversary activities in deception environments	Deception: Misdirection; Analytic Monitoring: Sensor Fusion and Analysis; Dynamic Representation: Dynamic Threat Modeling	Make the effects of deception and unpredictability user-transparent, Maintain situational awareness	EIT, LSPE, CPS	COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations)	Judged, Observed
UN-S1-A3-5	Average number of subsequent accesses by an adversary to a deception environment	Understand	Understand adversaries: Observe and analyze adversary activities in deception environments	Deception: Misdirection; Analytic Monitoring: Sensor Fusion and Analysis; Dynamic Representation: Dynamic Threat Modeling	Make the effects of deception and unpredictability user-transparent, Maintain situational awareness	EIT, LSPE, CPS	COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations)	Judged, Observed
UN-S1-A3-6	Number of times the adversary has positively identified/recognized the deception environment	Understand	Understand adversaries: Observe and analyze adversary activities in deception environments	Deception: Misdirection; Analytic Monitoring: Sensor Fusion and Analysis; Dynamic Representation: Dynamic Threat Modeling	Make the effects of deception and unpredictability user-transparent, Maintain situational awareness	EIT, LSPE, CPS	COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations)	Judged, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
UN-S1-A4-1	Percentage of high-value information assets which include hidden beaconing functionality	Understand	Understand adversaries: Reveal adversary data collection or exfiltration	Deception: Tainting	Make the effects of deception and unpredictability user-transparent	EIT, LSPE, CPS	COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations)	Judged, Observed
UN-S1-A4-2	Percentage of high-value information assets which include hidden signatures which make them discoverable via network searches	Understand	Understand adversaries: Reveal adversary data collection or exfiltration	Deception: Tainting	Make the effects of deception and unpredictability user-transparent	EIT, LSPE, CPS	COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations)	Judged, Observed
UN-S2-A1-1	Time since most recent update of MIA, BIA, or CJA	Understand	Understand dependencies on and among cyber resources: Perform impact analysis to identify critical assets / capabilities	Coordinated Protection: Consistency Analysis; Dynamic Representation: Dynamic Mapping and Profiling	Maintain situational awareness, Determine ongoing trustworthiness	EIT, LSPE, CPS	COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations), Social / Organizational	Judged, Observed
UN-S2-A1-2	Extent of validation of MIA, BIA, or CJA (e.g., review, tabletop exercise, COOP exercise)	Understand	Understand dependencies on and among cyber resources: Perform impact analysis to identify critical assets / capabilities	Coordinated Protection: Consistency Analysis; Dynamic Representation: Dynamic Mapping and Profiling	Maintain situational awareness, Determine ongoing trustworthiness	EIT, LSPE, CPS	COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations), Social / Organizational	Judged, Observed
UN-S2-A1-3	Percentage of cyber resources for which criticality has been determined	Understand	Understand dependencies on and among cyber resources: Perform impact analysis to identify critical assets / capabilities	Coordinated Protection: Consistency Analysis; Dynamic Representation: Dynamic Mapping and Profiling	Maintain situational awareness, Determine ongoing trustworthiness	EIT, LSPE, CPS	Engineering, COA Analysis, Investment / Programmatic	Cognitive (Cyber Operations), Social / Organizational	Judged, Computed or Derived
UN-S2-A2-1	Time required to refresh mission dependency map	Understand	Understand dependencies on and among cyber resources: Identify, and maintain a representation of, mission dependencies on cyber resources	Dynamic Representation: Dynamic Mapping and Profiling	Maintain situational awareness	EIT, LSPE, CPS	Engineering, Tactical Analysis, COA Analysis, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
UN-S2-A2-2	Time since most recent refresh of mission dependency map	Understand	Understand dependencies on and among cyber resources: Identify, and maintain a representation of, mission dependencies on cyber resources	Dynamic Representation: Dynamic Mapping and Profiling	Maintain situational awareness	EIT, LSPE, CPS	Engineering, Tactical Analysis, COA Analysis, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
UN-S2-A2-3	Degree of completeness of mission dependency map	Understand	Understand dependencies on and among cyber resources: Identify, and maintain a representation of, mission dependencies on cyber resources	Dynamic Representation: Dynamic Mapping and Profiling	Maintain situational awareness	EIT, LSPE, CPS	Engineering, Tactical Analysis, COA Analysis, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
UN-S2-A2-4	Percent of known cyber resources included in mission dependency map	Understand	Understand dependencies on and among cyber resources: Identify, and maintain a representation of, mission dependencies on cyber resources	Dynamic Representation: Dynamic Mapping and Profiling	Maintain situational awareness	EIT, LSPE, CPS	Engineering, Tactical Analysis, COA Analysis, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
UN-S2-A3-1	Time required to refresh functional dependency map	Understand	Understand dependencies on and among cyber resources: Identify, and maintain a representation of, mission dependencies on cyber resources	Dynamic Representation: Dynamic Mapping and Profiling	Maintain situational awareness	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Measured, Observed
UN-S2-A3-2	Time since most recent refresh of functional dependency map	Understand	Understand dependencies on and among cyber resources: Identify, and maintain a representation of, mission dependencies on cyber resources	Dynamic Representation: Dynamic Mapping and Profiling	Maintain situational awareness	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Measured, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
UN-S2-A3-3	Degree of completeness of functional dependency map	Understand	Understand dependencies on and among cyber resources: Identify, and maintain a representation of, mission dependencies on cyber resources	Dynamic Representation: Dynamic Mapping and Profiling	Maintain situational awareness	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged
UN-S2-A3-4	Percent of known cyber resources included in functional dependency map	Understand	Understand dependencies on and among cyber resources: Identify, and maintain a representation of, mission dependencies on cyber resources	Dynamic Representation: Dynamic Mapping and Profiling	Maintain situational awareness	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
UN-S2-A4-1	Time required to refresh external dependency map or inventory	Understand	Understand dependencies on and among cyber resources: Identify, and maintain a representation of, mission dependencies on cyber resources	Dynamic Representation: Dynamic Mapping and Profiling	Maintain situational awareness	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Measured, Observed
UN-S2-A4-2	Time since most recent refresh of external dependency map or inventory	Understand	Understand dependencies on and among cyber resources: Identify, and maintain a representation of, mission dependencies on cyber resources	Dynamic Representation: Dynamic Mapping and Profiling	Maintain situational awareness	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Measured, Observed
UN-S2-A4-3	Degree of completeness of external dependency map or inventory	Understand	Understand dependencies on and among cyber resources: Identify, and maintain a representation of, mission dependencies on cyber resources	Dynamic Representation: Dynamic Mapping and Profiling	Maintain situational awareness	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
UN-S2-A5-1	Time since last cyber table-top exercise, Red Team exercise, or execution of controlled automated disruption (e.g., via Simian Army)	Understand	Understand dependencies on and among cyber resources: Validate assumptions about dependencies and criticality by controlled disruption	Coordinated Protection: Self-Challenge	Determine ongoing trustworthiness	EIT, Federated EIT, LSPE, CPS, Federated CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed
UN-S2-A5-2	Frequency of cyber table-top exercises, Red Team exercises, or execution of controlled automated disruption	Understand	Understand dependencies on and among cyber resources: Validate assumptions about dependencies and criticality by controlled disruption	Coordinated Protection: Self-Challenge	Determine ongoing trustworthiness	EIT, Federated EIT, LSPE, CPS, Federated CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed
UN-S2-A6-1	Number of types of users for which degrees of trust are defined	Understand	Understand dependencies on and among cyber resources: Determine types and degrees of trust for users and cyber entities	Coordinated Protection: Consistency Analysis	Determine ongoing trustworthiness	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged
UN-S2-A6-2	Number of types of cyber entities for which degrees of trust are defined	Understand	Understand dependencies on and among cyber resources: Determine types and degrees of trust for users and cyber entities	Coordinated Protection: Consistency Analysis	Determine ongoing trustworthiness	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged
UN-S3-A2-1	Percentage of cyber resources monitored	Understand	Understand the status of resources with respect to threat events: Coordinate sensor coverage to minimize gaps or blind spots	Analytic Monitoring: Sensor Fusion and Analysis; Coordinated Protection: Orchestration	Determine ongoing trustworthiness, Leverage health and status data	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
UN-S3-A2-2	Percentage of types of cyber resources monitored	Understand	Understand the status of resources with respect to threat events: Coordinate sensor coverage to minimize gaps or blind spots	Analytic Monitoring: Sensor Fusion and Analysis; Coordinated Protection: Orchestration	Determine ongoing trustworthiness, Leverage health and status data	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged
UN-S3-A4-1	Percentage of those cyber resources monitored by more than one sensor	Understand	Understand the status of resources with respect to threat events: Correlate or otherwise combine data from different sensors	Analytic Monitoring: Sensor Fusion and Analysis	Determine ongoing trustworthiness, Leverage health and status data	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
UN-S3-A4-2	Number or percentage of sensors from which data is correlated or fused with data from other sensors	Understand	Understand the status of resources with respect to threat events: Correlate or otherwise combine data from different sensors	Analytic Monitoring: Sensor Fusion and Analysis	Leverage health and status data	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
UN-S3-A5-1	Percentage of cyber resources for which custom analytics have been developed	Understand	Understand the status of resources with respect to threat events: Develop custom analytics or sensors	Analytic Monitoring: Monitoring and Damage Assessment	Leverage health and status data	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
UN-S3-A6-1	Elapsed time for sensor reconfiguration to take effect	Understand	Understand the status of resources with respect to threat events: Dynamically reconfigure sensors	Adaptive Response: Dynamic Reconfiguration	Leverage health and status data	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Obserrved
UN-S3-A6-2	Percentage of sensors capable of being reconfigured	Understand	Understand the status of resources with respect to threat events: Dynamically reconfigure sensors	Adaptive Response: Dynamic Reconfiguration	Leverage health and status data	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
UN-S3-A7-1	Percentage of system elements for which failure or indication of potential faults can be detected	Understand	Understand the status of resources with respect to threat events: Perform damage assessment	Analytic Monitoring: Monitoring and Damage Assessment; Substantiated Integrity: Integrity Checks, Behavior Validation	Leverage health and status data	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
UN-S3-A7-2	Percentage of cyber resources for which damage can be assessed	Understand	Understand the status of resources with respect to threat events: Perform damage assessment	Analytic Monitoring: Monitoring and Damage Assessment; Substantiated Integrity: Integrity Checks, Behavior Validation	Leverage health and status data	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
UN-S3-A8-1	Time since last external search for evidence of exfiltrated data	Understand	Understand the status of resources with respect to threat events: Search externally for evidence of exfiltrated data	Analytic Monitoring: Monitoring and Damage Assessment; Deception: Tainting	Leverage health and status data	EIT, LSPE, CPS	Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed
UN-S3-A8-2	Number of external locations on which exfiltrated data are found	Understand	Understand the status of resources with respect to threat events: Search externally for evidence of exfiltrated data	Analytic Monitoring: Monitoring and Damage Assessment; Deception: Tainting	Leverage health and status data	EIT, LSPE, CPS	Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed
UN-S3-A9-1	Elapsed time between decision to relocate a sensor and delivery of initial sensor data	Understand	Understand the status of resources with respect to threat events: Dynamically relocate sensors	Dynamic Positioning: Functional Relocation of Sensors	Leverage health and status data	EIT, LSPE, CPS	Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
UN-S3-A10-1	Time to refresh the representation of the resiliency posture	Understand	Understand the status of resources with respect to threat events: Define and maintain a representation of the resiliency posture of cyber resources and adversary activities against cyber resources	Dynamic Representation: Mission Dependency and Status Visualization	Leverage health and status data	EIT, LSPE, CPS	Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured, Observed
UN-S3-A10-2	Percentage of critical resources represented in posture	Understand	Understand the status of resources with respect to threat events: Define and maintain a representation of the resiliency posture of cyber resources and adversary activities against cyber resources	Dynamic Representation: Mission Dependency and Status Visualization	Leverage health and status data	EIT, LSPE, CPS	Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
UN-S3-A10-3	Percentage of system resources represented in the resiliency posture representation	Understand	Understand the status of resources with respect to threat events: Define and maintain a representation of the resiliency posture of cyber resources and adversary activities against cyber resources	Dynamic Representation: Mission Dependency and Status Visualization	Leverage health and status data	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
UN-S3-A11-1	Percentage of mission-critical hardware components for which supply chain and assurance evidence is maintained	Understand	Understand the status of resources with respect to threat events: Validate provenance and quality of hardware and software	Substantiated Integrity: Provenance Tracking	Determine ongoing trustworthiness	EIT, LSPE, CPS	Engineering, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
UN-S3-A11-2	Percentage of mission-critical software components for which supply chain and assurance evidence is maintained	Understand	Understand the status of resources with respect to threat events: Validate provenance and quality of hardware and software	Substantiated Integrity: Provenance Tracking	Determine ongoing trustworthiness	EIT, LSPE, CPS	Engineering, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
UN-S3-A12-1	Percentage of mission-critical data assets for which data provenance measures have been implemented	Understand	Understand the status of resources with respect to threat events: Validate data provenance	Substantiated Integrity: Provenance Tracking	Determine ongoing trustworthiness	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
UN-S3-A12-2	Percentage of mission-critical data assets for which data provenance has been validated in the last [specify time period; will depend on mission tempo]	Understand	Understand the status of resources with respect to threat events: Validate data provenance	Substantiated Integrity: Provenance Tracking	Determine ongoing trustworthiness	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
UN-S3-A13-1	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]	Understand	Understand the status of resources with respect to threat events: Validate data integrity / quality to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks	Determine ongoing trustworthiness	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
UN-S3-A13-2	Percentage of mission-supporting data assets for which data integrity / quality has been validated in the last [specify time period; will depend on mission tempo]	Understand	Understand the status of resources with respect to threat events: Validate data integrity / quality to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks	Determine ongoing trustworthiness	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
UN-S3-A14-1	Percentage of mission-critical applications for which integrity / behavior has been validated in the last [specify time period; will depend on mission tempo]	Understand	Understand the status of resources with respect to threat events: Validate software / service integrity / behavior to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks, Behavior Validation	Determine ongoing trustworthiness	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
UN-S3-A14-2	Percentage of mission-supporting services for which integrity / behavior has been validated in the last [specify time period; will depend on mission tempo]	Understand	Understand the status of resources with respect to threat events: Validate software / service integrity / behavior to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks, Behavior Validation	Determine ongoing trustworthiness	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
UN-S3-A14-3	Frequency of software / service integrity check	Understand	Understand the status of resources with respect to threat events: Validate software / service integrity / behavior to ensure it has not been corrupted	Substantiated Integrity: Integrity Checks, Behavior Validation	Determine ongoing trustworthiness	EIT, LSPE, CPS	Engineering, Tactical Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
UN-S3-A15-1	Percentage of hardware components for which provenance can be tracked	Understand	Understand the status of resources with respect to threat events: Validate component integrity	Substantiated Integrity: Provenance Tracking	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
UN-S3-A15-2	Percentage of hardware components for which provenance actually is tracked	Understand	Understand the status of resources with respect to threat events: Validate component integrity	Substantiated Integrity: Provenance Tracking	Determine ongoing trustworthiness	EIT, LSPE, CPS, PIT	Engineering, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
TR-S1-A1-1	Percentage of mission threads which have been analyzed with respect to common dependencies and potential single points of failure	Transform	Redefine mission threads for agility: Identify and eliminate single points of failure in mission threads	Redundancy: Replication; Coordinated Protection: Consistency Analysis, Orchestration	Maintain redundancy	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
TR-S1-A1-2	Percentage of mission threads for which no single points of failure can be identified	Transform	Redefine mission threads for agility: Identify and eliminate single points of failure in mission threads	Redundancy: Replication; Coordinated Protection: Consistency Analysis, Orchestration	Maintain redundancy	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
TR-S1-A2-1	Percentage of mission threads for which alternative courses of action are documented	Transform	Redefine mission threads for agility: Identify and resource alternative mission courses of action	Coordinated Protection: Consistency Analysis, Orchestration	Plan and manage diversity, Maintain redundancy	EIT, Federated EIT, LSPE, CPS, Federated CPS, PIT	Engineering, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
TR-S1-A2-2	Percentage of staff identified in documented alternative courses of action who have been trained in those alternatives	Transform	Redefine mission threads for agility: Identify and resource alternative mission courses of action	Coordinated Protection: Consistency Analysis, Orchestration	Plan and manage diversity, Maintain redundancy	EIT, LSPE, CPS, PIT	Engineering, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations), Social / Organizational	Judged, Computed or Derived
TR-S1-A3-1	Percentage of services or processes which have been made non-persistent	Transform	Redefine mission threads for agility: Reduce the overhead and risk associated with persistent processing or communications	Non-Persistence: Non-Persistent Services, Non-Persistent Communications	Maximize transience	EIT, LSPE, CPS	Engineering	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
TR-S1-A3-2	Percentage of services or processes for which connectivity is established on-demand and dropped after transaction completion	Transform	Redefine mission threads for agility: Reduce the overhead and risk associated with persistent processing or communications	Non-Persistence: Non-Persistent Services, Non-Persistent Communications	Maximize transience	EIT, LSPE, CPS	Engineering	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
TR-S1-A3-3	Percentage of ports / protocols for which use is enabled on-demand and dropped after transaction completion	Transform	Redefine mission threads for agility: Reduce the overhead and risk associated with persistent processing or communications	Non-Persistence: Non-Persistent Services, Non-Persistent Communications	Maximize transience	EIT, LSPE, CPS	Engineering	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
TR-S2-A1-1	Percentage of mission threads for which no dependencies on resources shared with non-mission functions can be identified	Transform	Redefine mission / business functions to mitigate risks: Identify and mitigate unnecessary dependencies of mission threads on resources shared with non-mission functions	Realignment: Purposing	Limit the need for trust	EIT, LSPE, CPS	Engineering	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
TR-S2-A1-2	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	Transform	Redefine mission / business functions to mitigate risks: Identify and mitigate unnecessary dependencies of mission threads on resources shared with non-mission functions	Realignment: Purposing	Limit the need for trust	EIT, LSPE, CPS	Engineering	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
TR-S2-A2-1	Percentage of resources for which privilege requirements have been analyzed with respect to risk-benefit trade-offs	Transform	Redefine mission / business functions to mitigate risks: Reallocate resources and/or reassign administrative / management responsibility based on risk to mission / business function	Realignment: Restriction, Offloading; Coordinated Protection: Consistency Analysis, Orchestration	Limit the need for trust	EIT, LSPE, CPS	Engineering, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
TR-S2-A2-2	Percentage of problematic privilege assignments which have been changed since last analysis	Transform	Redefine mission / business functions to mitigate risks: Reallocate resources and/or reassign administrative / management responsibility based on risk to mission / business function	Realignment: Restriction, Offloading; Coordinated Protection: Consistency Analysis, Orchestration	Limit the need for trust	EIT, LSPE, CPS	Engineering, Tactical Operations	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
TR-S2-A3-1	Percentage of data feeds which have been analyzed (e.g., in terms of sources and protocols) with respect to risk-benefit trade-offs	Transform	Redefine mission / business functions to mitigate risks: Identify and remove or replace data feeds and connections for which risks outweigh benefits	Realignment: Restriction, Offloading	Limit the need for trust	EIT, LSPE, CPS	Engineering, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
TR-S2-A3-2	Percentage of problematic data feeds to which risk mitigations have been applied since last analysis	Transform	Redefine mission / business functions to mitigate risks: Identify and remove or replace data feeds and connections for which risks outweigh benefits	Realignment: Restriction, Offloading	Limit the need for trust	EIT, LSPE, CPS	Engineering, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
TR-S2-A4-1	Percentage of components which have been analyzed (e.g., in terms of supply chain or privilege requirements) with respect to risk-benefit trade-offs	Transform	Redefine mission / business functions to mitigate risks: Identify and remove or replace components for which risks outweigh benefits	Realignment: Specialization, Replacement	Limit the need for trust	EIT, LSPE, CPS	Engineering, Investment / Programmatic	Information / Technical, Social / Organizational	Judged, Computed or Derived
TR-S2-A4-2	Percentage of problematic components to which risk mitigations have been applied since last analysis	Transform	Redefine mission / business functions to mitigate risks: Identify and remove or replace components for which risks outweigh benefits	Realignment: Specialization, Replacement	Limit the need for trust	EIT, LSPE, CPS	Engineering, Investment / Programmatic	Information / Technical, Social / Organizational	Judged, Computed or Derived
TR-S2-A5-1	Percentage of data stores for which automated deletion / obfuscation has been implemented	Transform	Redefine mission / business functions to mitigate risks: Analyze data to assess lifespan / retention conditions and apply automated deletion / obfuscation	Non-Persistence: Non-Persistent Information	Maximize transience	EIT, LSPE, CPS	Engineering	Information / Technical	Judged, Computed or Derived
TR-S2-A5-2	Percentage of data stores for which lifespan / retention conditions have been analyzed	Transform	Redefine mission / business functions to mitigate risks: Analyze data to assess lifespan / retention conditions and apply automated deletion / obfuscation	Non-Persistence: Non-Persistent Information	Maximize transience	EIT, LSPE, CPS	Engineering	Information / Technical	Judged, Computed or Derived
RA-S1-A1-1	Percentage of cyber resources identified as critical assets (compared with same value at previous times or for prior spirals)	Re-architect	Restructure systems or sub-systems to reduce risks: Restructure systems or sub-systems to minimize the number of critical assets	Realignment: Purposing, Restriction	Limit the need for trust	EIT, LSPE, CPS	Engineering, Investment / Programmatic	Information / Technical	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
RA-S1-A2-1	Percentage of cyber resources which are non-persistent (compared with same value at previous times or for prior spirals)	Re-architect	Restructure systems or sub-systems to reduce risks: Restructure systems, sub-systems, or workflows to reduce the duration of exposures	Non-Persistence: Non-Persistent Information, Non-Persistent Services, Non-Persistent Connectivity	Maximize transience	EIT, LSPE, CPS	Engineering, Investment / Programmatic	Information / Technical	Judged, Computed or Derived
RA-S1-A3-1	Percentage of systems or sub-systems which can be repurposed or recomposed	Re-architect	Restructure systems or sub-systems to reduce risks: 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	Manage resources (risk-) adaptively	EIT, LSPE, CPS	Engineering, Investment / Programmatic	Information / Technical	Judged
RA-S1-A4-1	Size of the hardware attack surface	Re-architect	Restructure systems or sub-systems to reduce risks: 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	Limit the need for trust, Control visibility and use	EIT, LSPE, CPS	Engineering	Information / Technical	Judged, Computed or Derived
RA-S1-A4-2	Size of the software attack surface (using a well-defined method)	Re-architect	Restructure systems or sub-systems to reduce risks: 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	Limit the need for trust, Control visibility and use	EIT, LSPE, CPS	Engineering	Information / Technical	Judged, Measured, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
RA-S1-A4-3	Size of the supply chain attack surface	Re-architect	Restructure systems or sub-systems to reduce risks: Restructure systems or sub-systems to improve defensibility in the face of predicted long-term changes in adversary characteristics	Realignment: Specialization, Replacement, Offloading, Restriction; Segmentation: Predefined Segmentation	Limit the need for trust, Control visibility and use	EIT, LSPE, CPS, PIT	Engineering, Investment / Programmatic	Information / Technical, Social / Organizational	Judged
RA-S1-A4-4	Size of the general user attack surface	Re-architect	Restructure systems or sub-systems to reduce risks: Restructure systems or sub-systems to improve defensibility in the face of predicted long-term changes in adversary characteristics	Realignment: Specialization, Replacement, Offloading, Restriction; Segmentation: Predefined Segmentation	Limit the need for trust, Control visibility and use	EIT, LSPE, CPS, PIT	Engineering, Investment / Programmatic	Information / Technical, Social / Organizational	Judged, Measured, Computed or Derived
RA-S1-A4-5	Size of the privileged user attack surface	Re-architect	Restructure systems or sub-systems to reduce risks: Restructure systems or sub-systems to improve defensibility in the face of predicted long-term changes in adversary characteristics	Realignment: Specialization, Replacement, Offloading, Restriction; Segmentation: Predefined Segmentation	Limit the need for trust, Control visibility and use	EIT, LSPE, CPS, PIT	Engineering, Investment / Programmatic	Information / Technical, Social / Organizational	Judged, Measured, Computed or Derived
RA-S1-A4-6	Percentage of system components for which provenance can be determined	Re-architect	Restructure systems or sub-systems to reduce risks: Restructure systems or sub-systems to improve defensibility in the face of predicted long-term changes in adversary characteristics	Realignment: Specialization, Replacement, Offloading, Restriction; Segmentation: Predefined Segmentation	Limit the need for trust, Control visibility and use	EIT, LSPE, CPS, PIT	Engineering, Investment / Programmatic	Information / Technical	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
RA-S1-A4-7	Percentage of critical system components for which provenance can be determined	Re-architect	Restructure systems or sub-systems to reduce risks: Restructure systems or sub-systems to improve defensibility in the face of predicted long-term changes in adversary characteristics	Realignment: Specialization, Replacement, Offloading, Restriction; Segmentation: Predefined Segmentation	Limit the need for trust, Control visibility and use	EIT, LSPE, CPS, PIT	Engineering, Investment / Programmatic	Information / Technical	Judged, Computed or Derived
RA-S1-A4-8	Percentage of system components which can be selectively isolated	Re-architect	Restructure systems or sub-systems to reduce risks: Restructure systems or sub-systems to improve defensibility in the face of predicted long-term changes in adversary characteristics	Realignment: Specialization, Replacement, Offloading, Restriction; Segmentation: Predefined Segmentation	Limit the need for trust, Control visibility and use	EIT, LSPE, CPS, PIT	Engineering	Information / Technical	Judged, Computed or Derived
RA-S2-A1-1	Percentage of mission threads for which no dependencies on resources shared with non-mission functions can be identified	Re-architect	Modify systems or sub-systems to reduce risks: Identify and mitigate unnecessary dependencies of mission threads on resources shared with non-mission functions	Realignment: Purposing	Limit the need for trust	EIT, LSPE, CPS, PIT	Engineering	Information / Technical	Judged, Computed or Derived
RA-S2-A1-2	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	Re-architect	Modify systems or sub-systems to reduce risks: Identify and mitigate unnecessary dependencies of mission threads on resources shared with non-mission functions	Realignment: Purposing	Limit the need for trust	EIT, LSPE, CPS, PIT	Engineering	Information / Technical	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
RA-S2-A2-1	Percentage of resources for which privilege requirements have been analyzed with respect to risk-benefit trade-offs	Re-architect	Modify systems or sub-systems to reduce risks: Reallocate resources and/or reassign administrative / management responsibility based on risk to mission / business function	Realignment: Restriction, Offloading; Coordinated Protection: Consistency Analysis, Orchestration	Limit the need for trust	EIT, LSPE, CPS	Engineering	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
RA-S2-A2-2	Percentage of problematic privilege assignments which have been changed since last analysis	Re-architect	Modify systems or sub-systems to reduce risks: Reallocate resources and/or reassign administrative / management responsibility based on risk to mission / business function	Realignment: Restriction, Offloading; Coordinated Protection: Consistency Analysis, Orchestration	Limit the need for trust	EIT, LSPE, CPS	Engineering	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
RA-S2-A3-1	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)	Re-architect	Modify systems or sub-systems to reduce risks: Identify and remove or replace data feeds and connections for which risks outweigh benefits	Realignment: Restriction, Offloading	Limit the need for trust	EIT, LSPE, CPS	Engineering	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
RA-S2-A3-2	Percentage of problematic data feeds and connections to which risk mitigations have been applied since last analysis	Re-architect	Modify systems or sub-systems to reduce risks: Identify and remove or replace data feeds and connections for which risks outweigh benefits	Realignment: Restriction, Offloading	Limit the need for trust	EIT, LSPE, CPS	Engineering	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
RA-S2-A4-1	Percentage of components which have been analyzed (e.g., in terms of supply chain or privilege requirements) with respect to risk-benefit trade-offs	Re-architect	Modify systems or sub-systems to reduce risks: Identify and remove or replace components for which risks outweigh benefits	Realignment: Specialization, Replacement	Limit the need for trust	EIT, LSPE, CPS, PIT	Engineering	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
RA-S2-A4-2	Percentage of problematic components to which risk mitigations have been applied since last analysis	Re-architect	Modify systems or sub-systems to reduce risks: Identify and remove or replace components for which risks outweigh benefits	Realignment: Specialization, Replacement	Limit the need for trust	EIT, LSPE, CPS, PIT	Engineering	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
RA-S2-A5-1	Percentage of data stores for which automated deletion / obfuscation has been implemented	Re-architect	Modify systems or sub-systems to reduce risks: Analyze data to assess lifespan / retention conditions and apply automated deletion / obfuscation	Non-Persistence: Non-Persistent Information	Maximize transience	EIT, LSPE, CPS	Engineering	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
RA-S2-A5-2	Percentage of data stores for which lifespan / retention conditions have been analyzed	Re-architect	Modify systems or sub-systems to reduce risks: Analyze data to assess lifespan / retention conditions and apply automated deletion / obfuscation	Non-Persistence: Non-Persistent Information	Maximize transience	EIT, LSPE, CPS	Engineering	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
RA-S2-A6-1	Percentage of cyber resources for which custom analytics have been developed	Re-architect	Modify systems or sub-systems to reduce risks: Develop custom analytics or sensors	Analytic Monitoring: Monitoring and Damage Assessment	Leverage health and status data	EIT, LSPE, CPS	Engineering, Investment / Programmatic	Information / Technical	Judged

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
RA-S2-A7-2	Percentage of mission-critical components for which one or more custom-built alternatives are implemented	Re-architect	Modify systems or sub-systems to reduce risks: Re-implement critical components to reduce risks and provide alternative implementations	Diversity: Design Diversity, Synthetic Diversity, Path Diversity, Supply Chain Diversity; Realignment: Specialization, Replacement	Plan and manage diversity	EIT, LSPE, CPS	Engineering, Investment / Programmatic	Information / Technical	Judged
RA-S2-A7-3	Percentage of mission-critical components for which one or more alternative sources are available	Re-architect	Modify systems or sub-systems to reduce risks: Re-implement critical components to reduce risks and provide alternative implementations	Diversity: Design Diversity, Synthetic Diversity, Path Diversity, Supply Chain Diversity; Realignment: Specialization, Replacement	Plan and manage diversity	EIT, LSPE, CPS	Engineering, Investment / Programmatic	Information / Technical	Judged
RA-S2-A8-1	Number of different Information / Technical architecture standards for the same or similar capabilities used	Re-architect	Modify systems or sub-systems to reduce risks: 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	Plan and manage diversity	EIT, LSPE, CPS	Engineering, Investment / Programmatic	Information / Technical	Judged
RA-S2-A8-2	Percentage of critical data stores for which alternatives derived from different data sources are maintained	Re-architect	Modify systems or sub-systems to reduce risks: 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	Plan and manage diversity	EIT, LSPE, CPS	Engineering, Investment / Programmatic	Information / Technical	Judged

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
RA-S2-A8-3	Percentage of system resources for which alternatives from non-overlapping supply chains are maintained	Re-architect	Modify systems or sub-systems to reduce risks: 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	Plan and manage diversity	EIT, LSPE, CPS	Engineering, Investment / Programmatic	Information / Technical	Judged
MT-1	Percentage of cyber resources that are properly configured	Prevent / Avoid, Understand	Apply basic hygiene and risk-tailored controls: General, Understand the status of resources with respect to threat events: Track security posture of cyber resources (e.g., patch status, compliance with configuration guidance, distance to alert thresholds)	Analytic Monitoring: Monitoring and Damage Assessment	Leverage health and status data	EIT, LSPE, PIT, CPS	Administrative / Management, Tactical Operations	Cognitive (Cyber Operations)	Judged, Measured, Observed
MT-2	Number of attempted intrusions stopped at a network perimeter	Prevent / Avoid, Understand	Apply basic hygiene and risk-tailored controls: General; Understand the effectiveness of cyber security and cyber resiliency controls: Track effectiveness of defenses at different architectural locations	Analytic Monitoring: Monitoring and Damage Assessment	Leverage health and status data	EIT, LSPE, PIT, CPS	Tactical Operations	Cognitive (Cyber Operations)	Judged, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-4	Number of attempted intrusions deflected to a honeypot	Prevent / Avoid, Understand	Decrease the adversary's perceived benefits: Present misleading information about information, resources, and capabilities; Understand adversaries: Observe and analyze adversary activities in deception environments	Deception: Dissimulation, Misdirection	Make the effects of deception and unpredictability user-transparent	EIT, CPS	Tactical Operations	Cognitive (Cyber Operations)	Judged, Observed
MT-6	Length of time between an initial adversary act and its detection	Understand	Understand the effectiveness of cyber security and cyber resiliency controls: Track effectiveness of detection mechanisms at different architectural locations	Analytic Monitoring: Monitoring and Damage Assessment, Malware and Forensic Analysis	Leverage health and status data	EIT, PIT, Federated CPS	Tactical Operations	Cognitive (Cyber Operations)	Judged, Computed or Derived
MT-7	Percentage of mission-essential functions for which a procedural work-around is available	Prepare, Continue	Create and maintain CCoAs: 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	Diversity; Coordinated Protection: Consistency Analysis, Orchestration	Focus on Common Critical Assets	EIT, PIT, Federated CPS	COA Analysis	Cognitive (Mission Operations)	Judged
MT-8	Percentage of mission-essential capabilities for which two or more different instantiations are available	Prepare	Maintain the resources needed to execute cyber courses of action: Define and maintain determinably different alternative processing paths	Diversity: Design Diversity	Plan and manage diversity	EIT, LSPE, CPS	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-10	Additional / diverted level of effort to maintain mission-essential functions	Understand, Continue	Create and maintain cyber courses of action: Track effectiveness of CCoAs and adapt as necessary	Adaptive Response: Adaptive Management; Coordinated Protection: Consistency Analysis, Orchestration	Manage resources (risk-) adaptively	EIT, PIT, Federated CPS	COA Analysis, Investment / Programmatic	Cognitive (Mission Operations)	Judged
MT-12	Degree of degradation of a specific mission-essential function (or set of functions)	Continue	Minimize degradation of service delivery: Maintain acceptable levels of performance for mission-critical, security-critical, and mission-supporting applications and services	Adaptive Response: Adaptive Management; Dynamic Representation: Mission Dependency and Status Visualization	Manage resources (risk-) adaptively	EIT, PIT, Federated CPS	Tactical Operations, COA Analysis	Cognitive (Mission Operations)	Judged
MT-13	Length of time between initial disruption and availability (at minimum level of acceptability) of mission-essential functions	Constrain	Minimize degradation of service delivery: Maintain acceptable levels of performance for mission-critical, security-critical, and mission-supporting applications and services	Adaptive Response	Manage resources (risk-) adaptively	EIT, PIT, Federated CPS	COA Analysis	Cognitive (Mission Operations)	Judged, Computed or Derived
MT-14	Percentage of mission-essential datasets for which all items effectively have two or more independent external data feeds	Continue, Reconstitute	Maintain the resources needed to execute cyber courses of action: Identify and maintain determinably different mission data sources	Diversity, Redundancy	Plan and manage diversity	EIT, LSPE, PIT, Federated CPS	Engineering	Information / Technical	Judged, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-15	Percentage of data value assertions in a mission-essential data store for which two or more different data feeds are available	Continue, Reconstitute	Maintain the resources needed to execute cyber courses of action: Identify and maintain determinably different mission data sources	Diversity, Redundancy	Plan and manage diversity	EIT, LSPE, PIT, Federated CPS	Engineering	Information / Technical	Judged, Observed
MT-16	Percentage of mission-essential data stores for which a master copy exists	Prepare, Reconstitute	Maintain the resources needed to execute cyber courses of action: Create and maintain multiple protected instances of information	Diversity: Information Diversity; Redundancy: Replication	Maintain redundancy	EIT, LSPE, CPS	Engineering, Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Computed or Derived, Observed
MT-17	Percentage of data value assertions in a mission-essential data store for which a master copy exists	Prepare, Reconstitute	Maintain the resources needed to execute cyber courses of action: Create and maintain multiple protected instances of information	Diversity: Information Diversity; Redundancy: Replication	Maintain redundancy	EIT, LSPE, CPS	Engineering, Administrative / Management, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Computed or Derived, Observed
MT-20	Length of time between initial disruption and restoration	Reconstitute	Restore functionality: Execute recovery procedures in accordance with contingency or continuity of operations plans	Adaptive Response: Adaptive Management; Coordinated Protection: Orchestration; Redundancy: Protected Backup and Restore	Manage resources (risk-)adaptively	EIT, PIT, Federated CPS	Engineering, COA Analysis	Information / Technical	Judged, Computed or Derived
MT-21	Percentage of pre-disruption availability / performance after disruption	Continue, Reconstitute	Minimize degradation of service delivery: Maintain acceptable levels of performance for mission-critical, security-critical, and mission-supporting applications and services	Adaptive Response: Adaptive Management; Dynamic Representation: Mission Dependency and Status Visualization	Manage resources (risk-)adaptively	EIT, PIT, Federated CPS	Engineering, COA Analysis	Information / Technical	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-22	Quality of restored / recovered / reconstituted data	Reconstitute	Determine the trustworthiness of restored or reconstructed resources: Validate data integrity / quality of restored or reconstructed resources to ensure they not been corrupted	Substantiated Integrity: Integrity Checks	Manage resources (risk-)adaptively, Determine ongoing trustworthiness	EIT, PIT, Federated CPS	Engineering, COA Analysis	Information / Technical	Judged
MT-24	Percentage of data irrevocably lost due to an incident	Reconstitute, Understand	Understand the effectiveness of cyber security and cyber resiliency controls: Track effectiveness of CCoAs	Adaptive Response: Adaptive Management	Manage resources (risk-)adaptively, Determine ongoing trustworthiness	EIT, PIT, Federated CPS	Engineering, COA Analysis	Information / Technical	Judged
MT-26	Percentage of sub-systems or components redesigned to improve damage limitation	Re-Architect	Modify systems or sub-systems to reduce risks: Identify and remove or replace components for which risks outweigh benefits	Realignment: Specialization, Replacement	Limit the need for trust	EIT, LSPE, CPS, PIT	Engineering	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
MT-27	Number of new sensors installed	Re-Architect	Modify systems or sub-systems to reduce risks: Develop custom analytics or sensors	Analytic Monitoring: Monitoring and Damage Assessment	Limit the need for trust	EIT, LSPE, CPS	Engineering	Information / Technical, Cognitive (Cyber Operations)	Judged
MT-29	Length of time to deploy redundant resources	Continue, Reconstitute	Minimize interruptions in service delivery: Fail over to replicated resources	Adaptive Response: Dynamic Reconfiguration; Redundancy: Protected Backup and Restore, Replication	Manage resources (risk-)adaptively	EIT, LSPE, PIT, Federated CPS	Engineering	Cognitive (Mission Operations, Cyber Operations)	Judged, Measured
MT-31	Length of time to deploy a new instantiation of a required capability	Re-Architect	Modify systems or sub-systems to reduce risks: Re-implement critical components to reduce risks and provide alternative implementations	Diversity: Design Diversity, Synthetic Diversity, Path Diversity, Supply Chain Diversity; Realignment: Specialization, Replacement	Manage diversity, Change or disrupt the attack surface	EIT, LSPE, PIT, Federated CPS	Engineering, COA Analysis	Information / Technical, Cognitive (Cyber Operations)	Judged, Measured

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-33	Number of alternate instantiations of a required capability that can be deployed	Prepare	Maintain the resources needed to execute cyber courses of action: Define and maintain determinably different alternative processing paths	Diversity: Design Diversity	Plan and manage diversity	EIT, LSPE, CPS	Engineering, Tactical Operations, Investment / Programmatic	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
MT-35	Average length of time between the start of adversary activities and their discovery	Understand	Understand the effectiveness of cyber security and cyber resiliency controls: Track effectiveness of detection mechanisms at different architectural locations	Analytic Monitoring: Monitoring and Damage Assessment	Leverage health and status data	EIT, LSPE, PIT, Federated CPS	Tactical Operations	Cognitive (Cyber Operations)	Judged, Computed or Derived
MT-37	Average length of time to recover from incidents	Reconstitute	Restore functionality: Execute recovery procedures in accordance with contingency or continuity of operations plans	Adaptive Response: Adaptive Management; Coordinated Protection: Orchestration; Redundancy: Protected Backup and Restore	Manage resources (risk-) adaptively	EIT, LSPE, PIT, Federated CPS	Tactical Operations, COA Analysis	Cognitive (Mission Operations, Cyber Operations), Social / Organizational	Judged, Computed or Derived
MT-38	Average length of time to patch systems	Prevent / Avoid	Apply basic hygiene and risk-tailored controls	Coordinated Protection; Substantiated Integrity	Layer defenses and partition resources	EIT, LSPE, PIT, Federated CPS	Tactical Operations	Information / Technical	Measured, Observed, Computed or Derived
MT-39	Percentage of systems in compliance with organizationally mandated configuration guidance	Prevent / Avoid, Understand	Apply basic hygiene and risk-tailored controls: General, Understand the status of resources with respect to threat events: Track security posture of cyber resources (e.g., patch status, compliance with configuration guidance, distance to alert thresholds)	Analytic Monitoring: Monitoring and Damage Assessment	Layer defenses and partition resources	EIT, LSPE, PIT, Federated CPS	Tactical Operations	Information / Technical	Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-40	Percentage of information system security personnel that have received security training	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: General	Coordinated Protection	Layer defenses and partition resources	EIT, LSPE, PIT, Federated CPS	Investment / Programmatic	Social / Organizational	Measured, Observed, Computed or Derived
MT-41	Average length of time to patch network components	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: General	Coordinated Protection	Layer defenses and partition resources	EIT, LSPE, PIT, Federated CPS	Tactical Operations	Information / Technical	Measured, Observed, Computed or Derived
MT-42	Frequency of audit record analysis for inappropriate activity	Prevent / Avoid, Understand	Apply basic hygiene and risk-tailored controls: General, Understand the status of resources with respect to threat events: Track security posture of cyber resources (e.g., patch status, compliance with configuration guidance, distance to alert thresholds)	Analytic Monitoring: Monitoring and Damage Assessment	Leverage health and status data	EIT, LSPE, PIT, Federated CPS	Tactical Operations	Cognitive (Cyber Operations)	Measured, Observed
MT-44	Percentage of information systems for which annual testing of contingency plans has been conducted	Prepare, Continue	Create and maintain CCoAs: 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	Layer defenses and partition resources	EIT, Federated CPS	Investment / Programmatic	Social / Organizational	Measured, Observed
MT-46	Percentage of incidents reported within required timeframe per applicable incident category	Understand	Understand the effectiveness of cyber security and cyber resiliency controls: Track effectiveness of CCoAs	Analytic Monitoring, Adaptive Management	Maintain situational awareness	EIT, LSPE, PIT, Federated CPS	Tactical Operations	Cognitive (Cyber Operations)	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-47	Average length of time between the occurrence and the discovery of an anomaly	Understand	Understand the effectiveness of cyber security and cyber resiliency controls: Track effectiveness of detection mechanisms at different architectural locations	Analytic Monitoring: Monitoring and Damage Assessment	Maintain situational awareness, Leverage health and status data	EIT, LSPE, PIT, Federated CPS	Tactical Operations	Cognitive (Cyber Operations)	Judged, Computed or Derived
MT-49	Average length of time between cyber incidents	Understand	Understand the effectiveness of cyber security and cyber resiliency controls: Track effectiveness of defenses at different architectural locations	Analytic Monitoring: Monitoring and Damage Assessment	Maintain situational awareness	EIT, LSPE, PIT, Federated CPS	Tactical Operations	Cognitive (Cyber Operations)	Judged, Computed or Derived
MT-53	Average length of time for the organization to recover from damage caused by a cyber incident	Reconstitute, Understand	Understand the effectiveness of cyber security and cyber resiliency controls: Track effectiveness of CCoAs	Adaptive Response Adaptive Management; Analytic Monitoring: Monitoring and Damage Assessment; Redundancy: Protected Backup and Restore	Manage resources (risk-) adaptively	EIT, Federated EIT, LSPE, Federated CPS	Tactical Operations	Social / Organizational	Judged, Computed or Derived
MT-55	Percentage of managed systems checked for vulnerabilities in accordance with the organization's policy	Prevent / Avoid, Understand	Apply basic hygiene and risk-tailored controls; Understand the effectiveness of cyber security and cyber resiliency controls: Track effectiveness of detection mechanisms at different architectural locations	Analytic Monitoring: Monitoring and Damage Assessment	Maintain situational awareness, Leverage health and status data	EIT, LSPE, PIT	Tactical Operations	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
MT-56	Percentage of systems without “high” severity vulnerabilities based on Common Vulnerability Scoring System (CVSS) scoring	Prevent / Avoid	Apply basic hygiene and risk-tailored controls	Analytic Monitoring: Monitoring and Damage Assessment; Coordinated Protection: Consistency Analysis	Maintain situational awareness, Manage resources (risk-) adaptively	EIT, LSPE, PIT	Tactical Operations	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-57	Average length of time for the organization to mitigate identified vulnerabilities	Prevent / Avoid	Apply basic hygiene and risk-tailored controls	Coordinated Protection: Consistency Analysis	Manage resources (risk-) adaptively	EIT, LSPE, PIT	Tactical Operations	Information / Technical, Cognitive (Cyber Operations), Social / Organizational	Judged, Computed or Derived
MT-58	Percentage of managed systems for which an automated patch management process is used	Prevent / Avoid	Apply basic hygiene and risk-tailored controls	Coordinated Protection: Consistency Analysis	Manage resources (risk-) adaptively	EIT, LSPE, PIT	Tactical Operations	Information / Technical, Cognitive (Cyber Operations)	Measured, Observed
MT-60	Average length of time from patch release to patch installation	Prevent / Avoid	Apply basic hygiene and risk-tailored controls	Coordinated Protection: Consistency Analysis	Manage resources (risk-) adaptively	EIT, LSPE, PIT	Tactical Operations	Information / Technical, Cognitive (Cyber Operations)	Judged, Computed or Derived
MT-62	Percentage of systems for which a defined security configuration is required	Prevent / Avoid, Understand	Apply basic hygiene and risk-tailored controls: General, Understand the status of resources with respect to threat events: Track security posture of cyber resources (e.g., patch status, compliance with configuration guidance, distance to alert thresholds)	Analytic Monitoring: Monitoring and Damage Assessment; Coordinated Protection: Consistency Analysis	Layer defenses and partition resources	EIT, LSPE, PIT	Tactical Operations	Information / Technical, Cognitive (Cyber Operations)	Judged
MT-63	Percentage of personnel who successfully completed annual security training	Prevent / Avoid	Apply basic hygiene and risk-tailored controls	Coordinated Protection: Consistency Analysis	Layer defenses and partition resources	EIT, LSPE, PIT	Tactical Operations	Social / Organizational	Measured, Observed, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-65	Percentage of enterprise considered to be monitored effectively	Understand	Understand the effectiveness of cyber security and cyber resiliency controls: Track effectiveness of detection mechanisms at different architectural locations	Analytic Monitoring: Monitoring and Damage Assessment	Maintain situational awareness	EIT, LSPE, PIT	Engineering	Information / Technical, Cognitive (Cyber Operations)	Judged
MT-83	Percentage of classes of attacks that can be detected with existing means	Understand	Understand the effectiveness of cyber security and cyber resiliency controls: Track effectiveness of detection mechanisms at different architectural locations	Analytic Monitoring	Expect adversaries to evolve.	EIT, LSPE, PIT	Tactical Operations	Cognitive (Cyber Operations)	Judged
MT-85	Percentage of individually managed systems having a defined mode for degraded operation	Prepare, Continue	Create and maintain CCoAs: Define and implement automated CCoAs	Adaptive Response: Adaptive Management; Coordinated Protection: Orchestration	Manage resources (risk-)adaptively	EIT, LSPE, CPS, PIT	Tactical Operations	Information / Technical, Cognitive (Cyber Operations)	Judged
MT-86	Percentage of individually managed systems in which one or more resiliency techniques have been implemented	Re-Architect	Modify systems or sub-systems to reduce risks: General	Realignment	Reduce attack surfaces	EIT, LSPE, CPS, PIT	Engineering	Information / Technical	Judged
MT-89	Percentage of mission-essential processes and interfaces restored to pre-disruption state	Reconstitute	Restore functionality: Execute recovery procedures in accordance with contingency or continuity of operations plans	Adaptive Response: Adaptive Management; Coordinated Protection: Orchestration; Redundancy: Protected Backup and Restore	Manage resources (risk-)adaptively	EIT, LSPE, PIT	Tactical Operations	Cognitive (Mission Operations)	Judged, Measured, Computed or Derived
MT-90	Level of trust in a system that has been restored to its pre-disruption capability	Reconstitute	Determine the trustworthiness of restored or reconstructed resources	Substantiated Integrity: Integrity / Quality Checks	Limit the need for trust	EIT, LSPE, PIT	Tactical Operations	Cognitive (Mission Operations)	Judged

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-95	Degree of consistency between organizational threat-response policies for system managers and organizational threat-response policies for operators	Prepare, Transform	Create and maintain CCoAs: 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	Layer defenses and partition resources	EIT, LSPE, PIT	Engineering, Investment / Programmatic	Cognitive (Cyber Operations)	Judged
MT-98	Degree to which system operators deviate from documented cyber resiliency guidance and procedures	Prepare	Apply basic hygiene and risk-tailored controls	Coordinated Protection: Consistency Analysis	Layer defenses and partition resources	EIT, LSPE, PIT	Engineering, Investment / Programmatic	Cognitive (Cyber Operations)	Judged
MT-101	Percentage of red team attack scenarios where varying configurations of interrelated functions are subjected to attack	Understand	Understand dependencies on and among cyber resources: Validate assumptions about dependencies and criticality by controlled disruption	Coordinated Protection: Self-Challenge	Layer defenses and partition resources	EIT, LSPE, PIT	Engineering, COA Analysis	Cognitive (Cyber Operations)	Judged
MT-114	Percentage of security components that are monitored for communication between an adversary and their implanted malicious code	Understand	Understand the status of resources with respect to threat events: Validate software / service integrity / behavior to ensure it has not been corrupted	Substantiated Integrity: Behavior Validation	Assume compromised resources	EIT, LSPE, PIT	Investment / Programmatic, Tactical Operations	Information / Technical	Measured, Computed or Derived: Test, Field Operations
MT-115	Percentage of mission critical components that employ anti-tamper, shielding, and power line filtering	Reconstitute	Identify damage and untrustworthy resources: Identify damaged, corrupted, or subverted components	Coordinated Protection: Information / Technical Defense-in-Depth Realignment: Customization	Focus on common critical assets	EIT, LSPE, PIT,	Investment / Programmatic	Information / Technical	Measured, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-117	Percentage of mission critical components that are purpose built	Re-Architect	Modify systems or sub-systems to reduce risks: Re-implement critical components to reduce risks and provide alternative implementations	Diversity: Design Diversity, Synthetic Diversity, Path Diversity, Supply Chain Diversity; Realignment: Specialization, Replacement	Plan and manage diversity	EIT, LSPE, CPS	Engineering, Investment / Programmatic	Information / Technical	Judged
MT-121	Level of access limitation for external maintenance personnel	Prevent / Avoid	Apply basic hygiene and risk-tailored controls: General	Privilege Restriction: Privilege Management	Limit the need for trust	EIT, LSPE, PIT,	Investment / Programmatic	Cognitive (Cyber Operations)	Judged
MT-123	Percentage of administrators who can administer both network and security components	Prevent / Avoid	Modify configurations based on threat intelligence: Coordinate definition and assignment of privileges to eliminate opportunities for privilege	Privilege Restriction: Privilege Management	Limit the need for trust	EIT, LSPE, PIT	Investment / Programmatic	Cognitive (Cyber Operations)	Observed, Computed or Derived
MT-127	Percentage of Network Intrusion Detection Systems that are connected to the network using passive taps	Understand	Understand the status of resources with respect to threat events: Coordinate sensor coverage to mitigate adversary's attempts to thwart monitoring	Analytic Monitoring: Monitoring and Damage Assessment; Coordinated Protection: Orchestration; Deception: Obfuscation	Control visibility and use	EIT, LSPE, CPS: System includes and relies on intrusion detection system or tools	Engineering	Information / Technical	Judged, Observed
MT-129	Percentage of Network Intrusion Detection Systems that use an out-of-band network for remote management	Understand	Understand the status of resources with respect to threat events: Coordinate sensor coverage to mitigate adversary's attempts to thwart monitoring	Analytic Monitoring: Monitoring and Damage Assessment; Coordinated Protection: Orchestration; Deception: Obfuscation	Layer defenses and partition resources	EIT, LSPE, CPS: System includes and relies on intrusion detection system or tools	Engineering	Information / Technical	Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-131	Number or percentage of Network Intrusion Detection Systems that are implemented on separate platforms	Understand	Understand the status of resources with respect to threat events: Coordinate sensor coverage to mitigate adversary's attempts to thwart monitoring	Analytic Monitoring: Monitoring and Damage Assessment; Coordinated Protection: Orchestration; Deception: Obfuscation; Redundancy: Replication	Layer defenses and partition resources	EIT, LSPE, CPS: System includes and relies on intrusion detection system or tools	Engineering	Information / Technical	Observed, Computed or Derived
MT-132	Length of time to bring online a backup network intrusion detection system	Continue	Heighten protections during reconstitution: Intensify monitoring of restored or reconstructed resources	Redundancy: Protected Backup and Restore: Speed (applied to Analytic Monitoring capabilities)	Maintain redundancy	EIT, LSPE, CPS: System includes and relies on intrusion detection system or tools	Tactical Operations	Cognitive (Cyber Operations)	Measured, Observed
MT-133	Length of time packet capture and sniffing devices are connected to the network	Understand	Understand the status of resources with respect to threat events: Coordinate sensor coverage to mitigate adversary's attempts to thwart monitoring	Analytic Monitoring: Monitoring and Damage Assessment; Non-Persistence: Non-Persistent Connectivity	Maximize transience; minimize persistence Change or disrupt the attack surface	EIT, LSPE, CPS: System includes and relies on intrusion detection system or tools	Engineering	Information / Technical	Measured, Observed
MT-134	Percentage of DNS servers under the organization's control that have been hardened	Prevent / Avoid	Modify configurations based on threat intelligence	Realignment: Restriction	Contain and exclude behaviors	EIT, LSPE, PIT: System includes and relies on DNS server(s)	Engineering	Information / Technical	Judged
MT-135	Percentage of enterprise DNS servers to which Domain Name System Security (DNSSEC) extensions have been applied	Prevent / Avoid	Modify configurations based on threat intelligence	Realignment: Restriction	Contain and exclude behaviors	EIT, LSPE, PIT: System includes and relies on DNS server(s)	Engineering	Information / Technical	Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-136	Percentage of local enclaves configured with a DNS server	Constrain		Segmentation / Isolation: Predefined Segmentation	Control visibility and use	EIT, LSPE, PIT: System includes and relies on DNS server(s)	Investment / Programmatic	Information / Technical	Observed
MT-137	Number of platforms on which multiple DNS servers are co-hosted	Constrain		Segmentation / Isolation: Predefined Segmentation	Control visibility and use	EIT, LSPE, PIT: System includes and relies on DNS server(s)	Investment / Programmatic	Information / Technical	Observed
MT-138	Percentage of enterprise Active Directory servers that have hot swappable power supplies	Prepare		Redundancy: Replication	Maintain redundancy	EIT, LSPE, PIT: System includes and relies on Active Directory	Investment / Programmatic	Information / Technical	Observed
MT-139	Percentage of enterprise Active Directory servers that use RAID (Redundant Array of Independent Disks) drives	Prepare		Redundancy: Replication	Maintain redundancy	EIT, LSPE, PIT: System includes and relies on Active Directory	Investment / Programmatic	Information / Technical	Judged, Computed or Derived
MT-140	Frequency at which Active Directory is replicated when configured to use multi-master replication	Prepare		Redundancy: Replication	Maintain redundancy	EIT, LSPE, PIT: System includes and relies on Active Directory	Tactical Operations	Cognitive (Cyber Operations)	Measured, Computed or Derived
MT-141	Percentage of data centers across which Active Directory domain controllers are distributed where multi-master replication is used	Prepare		Redundancy: Replication	Maintain redundancy	EIT, LSPE, PIT: System includes and relies on Active Directory	Investment / Programmatic	Information / Technical	Judged, Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-142	Length of time to bring online an Active Directory warm backup domain controller	Continue, Reconstitute:		Redundancy: Replication	Maintain redundancy	EIT, LSPE, PIT: System includes and relies on Active Directory	Tactical Operations	Cognitive (Cyber Operations)	Measured, Computed or Derived
MT-143	Length of time to provide alternate email, file, and instant messaging service when the Active Directory (AD) authenticated services are disrupted	Continue, Reconstitute		Redundancy: Replication Diversity: Architectural Diversity / Heterogeneity	Plan and manage diversity	EIT, LSPE, PIT: System includes and relies on Active Directory	Tactical Operations	Cognitive (Cyber Operations)	Measured, Computed or Derived
MT-144	Percentage of the alternate email, file, and instant messaging services (response to AD denial) that are hosted on an OS platform other than Windows	Prepare, Continue		Redundancy: Replication Diversity: Architectural Diversity / Heterogeneity	Plan and manage diversity	EIT, LSPE, PIT: System includes and relies on Active Directory	Investment / Programmatic	Information / Technical	Judged, Computed or Derived
MT-151	Length of time for anomalous or malicious activity to be reported to an operator's console	Understand		Analytic Monitoring: Monitoring and Damage Assessment: Speed	Maintain situational awareness	EIT, LSPE, PIT	Tactical Operations	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed
MT-152	Percentage of anomalous or malicious events / behavior that can be associated with a person and a computing / communications device	Understand		Analytic Monitoring: Monitoring and Damage Assessment	Maintain situational awareness	EIT, LSPE, PIT	Tactical Operations	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-158	Number of alerts generated when routers or proxies detect attempts to send packets directly to a hidden client	Understand		Analytic Monitoring: Monitoring and Damage Assessment	Maintain situational awareness	EIT, LSPE, PIT	Tactical Operations	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed
MT-159	Length of time to bring a backup server online	Continue, Reconstitute	Minimize interruptions in service delivery: Fail over to replicated resources	Adaptive Response: Dynamic Reconfiguration; Redundancy: Protected Backup and Restore, Replication	Manage resources (risk-)adaptively	EIT, LSPE, PIT	Tactical Operations	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed
MT-160	Length of time for detailed information about a system to be delivered to an operator who has requested it in response to an alert	Understand	Understand the status of resources with respect to threat events: Track security posture of cyber resources (e.g., patch status, compliance with configuration guidance, distance to alert thresholds)	Analytic Monitoring: Monitoring and Damage Assessment	Maintain situational awareness	EIT, LSPE, PIT	Tactical Operations	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed
MT-176	Length of time to report packets to/from an invalid port on a server	Understand		Analytic Monitoring: Monitoring and Damage Assessment	Leverage health and status data	EIT, LSPE, PIT	Tactical Operations	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed
MT-177	Length of time to report attempts to access unauthorized ports or inaccessible addresses	Understand	Understand the status of resources with respect to threat events: Track security posture of cyber resources (e.g., patch status, compliance with configuration guidance, distance to alert thresholds)	Analytic Monitoring: Monitoring and Damage Assessment	Leverage health and status data	EIT, LSPE, PIT	Tactical Operations	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-178	Length of time to report attempts at IP address spoofing	Understand	Understand the status of resources with respect to threat events: Track security posture of cyber resources (e.g., patch status, compliance with configuration guidance, distance to alert thresholds)	Analytic Monitoring: Monitoring and Damage Assessment	Leverage health and status data	EIT, LSPE, PIT	Tactical Operations	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed
MT-179	Length of time for packets to un-routable IP addresses to be reported	Understand	Understand the status of resources with respect to threat events: Track security posture of cyber resources (e.g., patch status, compliance with configuration guidance, distance to alert thresholds)	Analytic Monitoring: Monitoring and Damage Assessment	Leverage health and status data	EIT, LSPE, PIT	Tactical Operations	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed
MT-180	Length of time for packets to/from an invalid port on a server to be reported	Understand	Understand the status of resources with respect to threat events: Track security posture of cyber resources (e.g., patch status, compliance with configuration guidance, distance to alert thresholds)	Analytic Monitoring: Monitoring and Damage Assessment	Leverage health and status data	EIT, LSPE, PIT	Tactical Operations	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed
MT-181	Percentage of unauthorized changes to row data in a database that are detected	Understand	Understand the status of resources with respect to threat events: Validate data integrity / quality to ensure it has not been corrupted	Substantiated Integrity: Integrity / Quality Checking	Determine ongoing trustworthiness	EIT, LSPE, PIT	Tactical Operations	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-183	Frequency at which key information assets are replicated to a backup data store or standby system through database journaling	Prepare	Create and maintain cyber courses of action: Back up data needed to restore or reconstitute mission and supporting functionality	Redundancy: Protected Backup and Restore	Maintain redundancy	EIT, LSPE, CPS	Tactical Operations, Administrative / Management, Investment / Programmatic	Cognitive (Cyber Operations)	Computed or Derived, Measured, Observed
MT-184	Length of time to reconstitute a key information asset from a backup data store	Reconstitute	Restore functionality: Execute recovery procedures in accordance with contingency or continuity of operations plans	Adaptive Response: Adaptive Management; Coordinated Protection: Orchestration; Redundancy: Protected Backup and Restore	Manage resources (risk-)adaptively	EIT, LSPE, PIT	Tactical Operations	Cognitive (Cyber Operations)	Computed or Derived
MT-189	Length of time to locate tools, services, and data sources needed to repair or reconstitute an infrastructure that serves mission requirements	Reconstitute	Restore functionality: Reconstruct compromised critical assets or capabilities from existing resources	Adaptive Response: Dynamic Reconfiguration: Speed; Realignment: Repurposing: Speed	Manage resources (risk-)adaptively	EIT, LSPE, PIT	Tactical Operations	Cognitive (Cyber Operations)	Computed or Derived
MT-192	Length of time to combine tools, services, and data sources needed to repair or reconstitute the infrastructure that serves mission requirements	Reconstitute	Restore functionality: Reconstruct compromised critical assets or capabilities from existing resources	Adaptive Response: Dynamic Reconfiguration: Speed; Realignment: Repurposing: Speed	Manage resources (risk-)adaptively	EIT, LSPE, PIT	Tactical Operations	Cognitive (Cyber Operations)	Computed or Derived
MT-195	Length of time to put into operational use the tools, services, and data sources needed to repair or reconstitute the infrastructure that serves mission requirements	Reconstitute	Restore functionality: Reconstruct compromised critical assets or capabilities from existing resources	Adaptive Response: Dynamic Reconfiguration: Speed; Realignment: Repurposing: Speed	Manage resources (risk-)adaptively	EIT, LSPE, PIT	Tactical Operations	Cognitive (Cyber Operations)	Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-202	Percentage of virtual machine (VM) images available for download for which alternative codebases exist	Prepare		Diversity: Synthetic Diversity, Design Diversity / Heterogeneity	Plan and manage diversity	EIT, LSPE	Tactical Operations	Cognitive (Cyber Operations)	Measured, Computed or Derived
MT-216	Length of time to change a software image to a different one of equivalent functionality	Continue		Adaptive Response: Dynamic Reconfiguration: Speed	Manage resources (risk-)adaptively	EIT, LSPE	Tactical Operations	Cognitive (Cyber Operations)	Computed or Derived
MT-218	Percentage of deployed software for which updates are tracked using OVAL definitions	Prevent / Avoid		Adaptive Response: Dynamic Reconfiguration	Manage resources (risk-)adaptively	EIT, LSPE	Tactical Operations	Cognitive (Cyber Operations)	Computed or Derived
MT-227	Length of time to redirect specific network packets to an alternate destination (i.e., not dictated by the destination addresses in the packets) in response to a detected threat or attack	Prevent / Avoid, Constrain		Adaptive Response: Dynamic Reconfiguration: Speed	Manage resources (risk-)adaptively	EIT, LSPE, PIT, CPS	Tactical Operations	Information / Technical	Computed or Derived
MT-228	Length of time to redirect all network packets to a pre-configured alternate destination (i.e., not dictated by the destination addresses in the packets)	Prevent / Avoid, Constrain		Adaptive Response: Dynamic Reconfiguration: Speed	Manage resources (risk-)adaptively	EIT, LSPE, PIT, CPS	Tactical Operations	Information / Technical	Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-230	Length of time to automatically redirect network packets to an alternate destination based on established / evolving packet redirection rules (i.e., not dictated by the destination addresses in the packets)	Prevent / Avoid, Constrain, Transform		Adaptive Response: Dynamic Reconfiguration: Speed	Support agility and architect for adaptability	EIT, LSPE, PIT, CPS		Information / Technical	Measured, Computed or Derived
MT-238	Length of time for network packets selected by sensor module analytics to be redirected to a different destination (i.e., not the destination address in the packet) as a result of evolving packet redirection rules	Transform		Adaptive Response: Dynamic Reconfiguration: Speed	Support agility and architect for adaptability	EIT, LSPE, PIT, CPS	Tactical Operations	Information / Technical	Measured, Computed or Derived
MT-240	Number of packets intended to be redirected by a new rule that make it on to the internal network before the new rule is in force	Prevent / Avoid, Constrain, Transform		Adaptive Response: Dynamic Reconfiguration	Support agility and architect for adaptability	EIT, LSPE, PIT, CPS	Tactical Operations	Information / Technical	Observed, Computed or Derived
MT-263	Length of time to reconstitute a database table from a backup data store	Reconstitute		Redundancy: Protected Backup and Restore: Speed	Maintain redundancy	EIT, LSPE, PIT, CPS	Engineering	Cognitive (Cyber Operations)	Computed or Derived, Judged
MT-264	Length of time an attacker remains contained in a deception environment	Understand	Understand adversaries: Observe and analyze adversary activities in deception environments	Deception: Misdirection / Simulation	Make unpredictability and deception user-transparent	EIT, CPS	COA Analysis	Cognitive (Cyber Operations)	Computed or Derived, SME analysis

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-265	Percentage of attackers in a deception environment who are unaware of their containment	Understand	Understand adversaries: Observe and analyze adversary activities in deception environments	Deception: Misdirection / Simulation	Make unpredictability and deception user-transparent	EIT, CPS	COA Analysis	Cognitive (Cyber Operations)	Computed or Derived, Judged
MT-266	Percentage of times attacker goals can be discerned from activities in a deception environment	Understand	Understand adversaries: Observe and analyze adversary activities in deception environments	Deception: Misdirection / Simulation	Make unpredictability and deception user-transparent	EIT, CPS	COA Analysis	Cognitive (Cyber Operations)	Computed or Derived, Judged
MT-267	Percentage of times an attacker in a deception environment closes out their encounter normally (i.e., removes traces of activity)	Understand	Understand adversaries: Observe and analyze adversary activities in deception environments	Deception: Misdirection / Simulation	Make unpredictability and deception user-transparent	EIT, CPS	COA Analysis	Cognitive (Cyber Operations)	Computed or Derived, Judged
MT-268	Length of time to determine what impact a cyber attack has had on a mission	Understand		Dynamic Representation: Mission Dependency and Status Visualization	Maintain situational awareness	EIT, LSPE, PIT, CPS	COA Analysis	Cognitive (Cyber Operations)	Computed or Derived, Judged
MT-269	Length of time between when a defensive response is selected and when a mission capability is restored	Reconstitute		Adaptive Response, Coordinated Protection	Layer defenses and partition resources	EIT, LSPE, PIT, CPS	COA Analysis	Cognitive (Cyber Operations and Mission Operations)	Computed or Derived, Judged
MT-270	Percentage of critical incident types for which pre-planned responses exist	Prepare		Coordinated Protection	Focus on common critical assets	EIT, LSPE, PIT, CPS	COA Analysis	Cognitive (Cyber Operations)	Judged
MT-271	Length of time a mission is negatively affected after an attack	Reconstitute		Adaptive Response, Coordinated Protection	Manage resources (risk-) adaptively	EIT, LSPE, PIT, CPS	COA Analysis	Cognitive (Mission Operations)	Computed or Derived

Identifier	Descriptor / Name	Cyber Resiliency Objective(s)	Sub-Objectives and Activities	Cyber Resiliency Technique(s) or Approach(es)	Cyber Resiliency Design Principle(s)	Type(s) of System	Type(s) of Decisions Supported	Domain	How Obtained
MT-272	Length of time from opening of a trouble report to closing of the trouble report	Prevent / Avoid		Coordinated Protection	Layer defenses and partition resources	EIT, LSPE, PIT, CPS	Investment / Programmatic	Cognitive (Cyber Operations)	Computed or Derived
ST-2-1	Time needed for an external entity to determine whether the system responds to a given type of query	Prevent / Avoid	Decrease the adversary's perceived benefits	Privilege Restriction, Segmentation	Control visibility and use: Restrict external visibility of system behaviors	EIT, LSPE, CPS	Engineering, Tactical Operations	Information / Technical, Cognitive (Cyber Operations)	Observed, Computed or Derived
ST-2-2	Time needed for an external entity to estimate system load based on latency in response to queries	Prevent / Avoid	Decrease the adversary's perceived benefits	Privilege Restriction, Segmentation	Control visibility and use: Restrict external visibility of system behaviors	EIT, LSPE, CPS	Engineering, Tactical Operations	Information / Technical, Cognitive (Cyber Operations)	Observed, Computed or Derived

Appendix B Acronyms

AD	Active Directory
APT	Advanced Persistent Threat
ATT&CK™	Adversarial Tactics, Techniques & Common Knowledge
CCoA	Cyber Course of Action
CIO	Chief Information Officer
COA	Course of Action
CPS	Cyber-Physical System
CR	Cyber Resiliency
CRDP	Cyber Resiliency Design Principles
CREF	Cyber Resiliency Engineering Framework
DNS	Domain Name Service
DoD	Department of Defense
DON	Department of the Navy
EIT	Enterprise IT
FISMA	Federal Information Security Management Act
IdAM	Identity and Access Management
IP	Internet Protocol
IT	Information Technology
LSPE	Large-Scale Processing Environment
M&S	Modeling and Simulation
MBSE	Model-Based Systems Engineering
MECR	Measuring the Effectiveness of Cyber Resiliency
MIP	MITRE Innovation Program
MOE	Measure of Effectiveness
MOP	Measure of Performance
MTR	MITRE Technical Report
NIST	National Institute of Standards and Technology
OS	Operating System
OVAL®	Open Vulnerability and Assessment Language
PIT	Platform IT
RAID	Redundant Array of Independent Disks
SME	Subject Matter Expert
SP	[NIST] Special Publication
SSM-CR	Situated Scoring Methodology for Cyber Resiliency

TTP	Tactic, Technique, or Procedure
TTPs	Tactics, Techniques, and Procedures
VM	Virtual Machine