MITRE

MTR210700R1
MITRE TECHNICAL REPORT

Cyber Resiliency Framework and Cyber Survivability Attributes

Mapping Cyber Resiliency to the CSEIG CSAs (Revision 1)

Sponsor: National Institute of Standards and Technology (NIST) National Cybersecurity Center of Excellence (NCCoE) in partnership with Air Force Research Laboratory Information Directorate (AFRL/RI)
Dept. No.: L522
Contract No.: SB-1341-14-CQ-0010
Project No.: 2721NT84-CR, and 54AOH760-CA

Author(s):
Ellen R. Laderman
Deborah J. Bodeau
Richard D. Graubart
Linda K. Jones

September2022

Bedford, MA

Abstract

Cyber survivability – defined in the *Cyber Survivability Endorsement Implementation Guide (CSEIG)* for weapon systems and defense critical infrastructure systems – aligns with cyber resiliency as defined in NIST SP 800-160 Vol. 2. Numerous controls in NIST SP 800-53 Rev. 5 have been identified as supporting cyber resiliency. This report maps cyber resiliency constructs – cyber resiliency design principles, techniques, implementation approaches, and controls to the CSAs defined by the CSEIG, to identify controls which support specific CSAs. While the mapping tables presented here can be used directly by systems engineers, the mappings have also been incorporated into the Air Force Research Laboratory's (AFRL's) CSA Tool, which enables systems engineers to identify, evaluate gaps in, and make trade-offs among system security controls.

Acknowledgments

The authors gratefully acknowledge and appreciate the contributions from Jim Reilly of the Air Force Research Laboratory, Rebecca Onuskanich of International Cyber Institute, Kenneth Colerick of Alluvion Data Solutions, Jason Rice of Quanterion Solutions, Amy Heburn of PAR Government Systems, Dr. Ron Ross of the National Institute of Standards and Technology, Ray Bongiorni of NSA, Steve Pitcher, Tom Andress and James Brown of Joint Staff/J-6, and Brian Abe, David Black, John Mulvihill, and Beverly Ware of the MITRE Corporation. The authors are also grateful to MITRE's National Cybersecurity Division and the Space Systems Integration Office at Space Systems Command for support to produce this report.

Table of Contents

List of Figures

List of Tables

1 Introduction

The Cyber Survivability Endorsement Implementation Guide (CSEIG, [1]) directs that weapon systems and defense critical infrastructure systems demonstrate *the ability to prevent, mitigate, recover from, and adapt to adverse cyber events that could impact mission related functions, by applying a risk managed approach to achieve and maintain an operationally relevant risk posture, throughout the system lifecycle* [2]. For such systems, Cyber Survivability Attributes (CSAs) must be selected and tailored to the system in its operational and threat environment, so that the system can be demonstrated to provide adequate survivability. Simultaneously, Department of Defense (DoD) systems must be demonstrated to provide adequate cybersecurity via the Risk Management Framework (RMF, [3]). To apply the RMF, systems engineers for such systems need to select controls[1] from NIST SP 800-53. Numerous controls in NIST SP 800-53 Rev. 5 [4] have been identified as supporting cyber resiliency, as defined in NIST SP 800-160 Vol. 2 [5] [6]: *the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources*. Despite differences in scope, cyber survivability aligns closely with cyber resiliency [2]. Therefore, the cyber resiliency controls are a logical starting point for identifying controls which support cyber survivability.

This report provides an initial mapping of cyber resiliency constructs – cyber resiliency design principles, techniques, implementation approaches, and controls to the CSAs defined by the CSEIG, to identify controls which support specific CSAs. The identification of cyber resiliency controls supporting CSAs have also been incorporated into the Air Force Research Laboratory's (AFRL's) CSA Tool, which enables systems engineers to identify, evaluate gaps in, and make trade-offs among system security controls. The tables in this report are intended to help systems engineers understand the rationale behind the identification of cyber resiliency controls in the CSA Tool, by providing a starting point to answer the question:

> *Which cyber resiliency design principles, techniques, implementation approaches, and controls can be used to support the adequate implementation of a given Cyber Survivability Attribute?*

It should be noted that the implementation of a CSA will also involve security controls which are not identified as cyber resiliency-related. While mappings of non-cyber resiliency controls have been performed and incorporated into the CSA Tool, such mappings are outside the scope of this report. It must also be noted that the initial mapping in this report is subject to caveats (see Section 2.3) and should not be used without careful engineering analysis to ensure that the selection and tailoring of controls for a system will be consistent with the system's operational, technical, and mission constraints.

The work presented in this report is an update and expansion of a prior mapping of cyber resiliency to cyber survivability [7]. That mapping described a process for identifying controls based on relationships between cyber resiliency constructs (design principles, techniques, and approaches) and the CSAs, but did not identify controls. This update and expansion are based on work for NIST and AFRL and includes the updates based on NIST SP 800-160 Vol. 2 R1 [6] and NIST SP 800-53 R5 [4].

[1] The term controls throughout this report refers to both controls and control enhancements defined in NIST SP 800-53.

The rest of this Introduction provides background on cyber resiliency, cyber survivability, and the AFRL CSA Tool. Section 2 describes the analysis process used to produce the mapping tables, which are presented in Section 3. Several appendices are included for the reader's convenience: definitions of cyber resiliency constructs, relationships between constructs, and a list of cyber resiliency controls identifying the CSAs they support, all based on NIST SP 800-160 Vol. 2 R1 [6]. Appendix D provides exemplar language for the CSAs from Section 13 of the CSEIG [1].

1.1 Cyber Resiliency

NIST SP 800-160 Vol. 2 R1 [6] defines **cyber resiliency** as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources." This definition was crafted, based on a variety of other definitions of resilience-related terms, to be applicable to range of subjects, including a system; a mechanism, component, or system element; a shared service, common infrastructure, or system-of-systems identified with a mission or business function; an organization; a critical infrastructure sector or a region; a system-of-systems in a critical infrastructure sector or sub-sector; and the Nation. Cyber resiliency can also be a property of a mission, business function, or a constituent task of a mission or business function. This interpretation relies on treating the task, business function, or mission as a socio-technical system (or system-of-systems). Cyber resiliency engineering builds on cybersecurity as well as other engineering disciplines, e.g., safety, reliability, or performance engineering, and is closely related to cyber survivability [7].

As illustrated in Figure 1, different constructs are used to describe (i) the cyber resiliency problem domain – the "what" of cyber resiliency (what properties, behaviors, and capabilities are needed, based on the risk management strategy) and (ii) the cyber resiliency solution domain – the "how" of cyber resiliency (how to select and use technologies, practices, processes, and products). Constructs describing "what" – goals and objectives – are consistent with Resilience Engineering [8] and the NIST Cybersecurity Framework [9]. Constructs describing "how" include design principles, techniques, and implementation approaches. These "how" constructs are informed by other specialty engineering disciplines, including system survivability, reliability, and security.

NIST SP 800-160 Vol. 2 R1 identifies controls, as defined in NIST SP 800-53 R5 [4], which directly support cyber resiliency. These controls, as listed in Table E-1 of [6], apply one or more of the implementation approaches to the cyber resiliency techniques. A version of this table is reproduced in Appendix C. For reference, the strategic design principles, structural design principles, techniques and implementation approaches are summarized in Appendix A of this report.

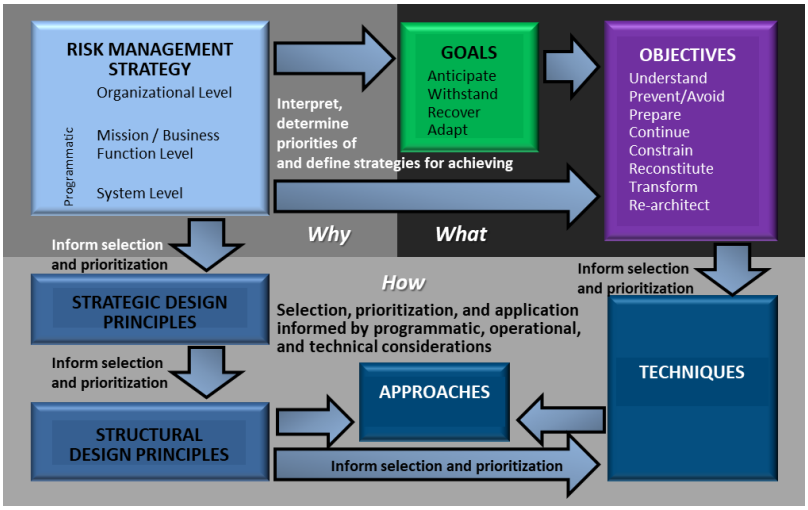

Figure 1. Cyber Resiliency Engineering Framework (CREF) (derived from [6])

1.2 Cyber Survivability Attributes

Cyber survivability is defined as the ability of warfighter systems to prevent, mitigate, recover from, and adapt to adverse cyber-events that could impact mission related functions, by applying a risk managed approach to achieve and maintain an operationally relevant risk posture, throughout the system lifecycle [1]. The CSEIG articulates cyber survivability requirements to satisfy the Joint Capabilities Integration and Development System (JCIDS) System Survivability Key Performance Parameter (SS KPP). The cyber survivability attributes ensure systems are designed to prevent, mitigate, recover from, and adapt to cyber-attacks [10]. The CSEIG leverages the NIST Cybersecurity Framework, JCIDS SS KPP, the RMF, and cyber threat intelligence.

Table 1 summarizes the ten CSAs, grouping them by SS KPP pillar. The "Prevent" KPP pillar is focused on anticipating what the adversary might do and putting in place mechanisms to prevent or avoid it. The "Mitigate" KPP pillar is associated with withstanding the adversary's activities. These attributes focus on mechanisms and configurations put in place to be used during an adverse event. The "Recover" KPP pillar is associated with recovering from attacks and is more dependent on process and policy than the other two SS KPP pillars. Each KPP pillar builds on the preceding group. All can be supported and strengthened by cyber resiliency guidance.

Table 1. Cyber Survivability Attributes and System Survivability KPP Pillars

System Survivability KPP Pillar	Cyber Survivability Attributes (CSAs) from the CSEIG
Prevent	CSA-01 – Control Access
	CSA-02 – Reduce System's Cyber Detectability
	CSA-03 – Secure Transmissions and Communications
	CSA-04 – Protect System's Information from Exploitation
	CSA-05 – Partition and Ensure Critical Functions at Mission Completion Performance Levels
	CSA-06 – Minimize and Harden Attack Surfaces
Mitigate	CSA-07 – Baseline & Monitor Systems and Detect Anomalies
	CSA-08 – Manage System Performance and Enable Cyberspace Defense
Recover	CSA-09 – Recover System Capabilities
Adapt for Prevent, Mitigate and Recover	CSA 10 – Actively Manage System's Configurations to Achieve and Maintain an Operationally-Relevant Cyber Risk Posture

The exemplar language for each CSA is replicated from the CSEIG [1] in the relevant subsections of Section 3.

1.3 AFRL CSA Tool

The AFRL CSA Tool provides its users – systems engineers, test engineers, acquisition personnel, and Program Office staff – with a customizable workflow process tool for analyzing and making trade-offs among security controls. The CSA Tool, which has Joint Staff advocacy, incorporates a database containing much of the existing Risk Management Framework (RMF) and Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253 guidance, as well as the CSEIG [1].

The CSA Tool includes a complete mapping for each of the ten CSAs to cyber resiliency objectives, techniques, and approaches from NIST SP 800-160 Vol. 2 R1 [6], to NIST SP 800-53 Revision 4 and Revision 5 security controls. The CSA Tool also identifies the effects those cyber resiliency approaches and security controls could be expected to have on adversary tactics and techniques from the community driven, Cyber Threat Intelligence (CTI) framework known as Adversary Tactics Techniques and Common Knowledge® (ATT&CK®), based on mappings in NIST SP 800-160 Vol. 2 R1 and a MITRE document mapping cyber resiliency to the ATT&CK® framework [11]. The tool has a recently updated database which contains information about and relationships between:

- NIST SP 800-37, the Risk Management Framework (RMF) [4], and DoDI 8510.01, the DoD version of the RMF
- NIST SP 800-53 R5 [4] and its predecessor NIST SP 800-53 R4 [12]
- The Cyber Resiliency Framework (NIST SP 800-160 Vol. 2), mapped to security controls in NIST SP 800-53 R5 (i.e., cyber resiliency controls)
- The CSAs defined in the CSEIG, mapped to cyber resiliency and non-cyber resiliency security controls from NIST SP 800-53 R4/R5 that support the CSAs
- ATT&CK® https://attack.mitre.org/versions/v9/, mapped to cyber resiliency approaches and security controls[2]
- Effects of cyber resiliency techniques on adversarial threat events
- Committee on National Security Systems (CNSS) Instruction (CNSSI) 1253 [13] guidance, to include controls and enhancements from NIST SP 800-53 R4
- NIST SP 800-53R4 baselines
- CNSSI 1253 baselines (using NIST SP 800-53 R4)
- Approved NIST and CNSSI overlays along with some unofficial, but useful, agency and department developed overlays

[2] The CSA Tool includes the mappings of cyber resiliency approaches and controls to ATT&CK for Enterprise and ATT&CK for Industrial Control Systems (ICS) from NIST SP 800-160 Vol. 2 R1. The CSA Tool also includes mappings of non-cyber resiliency controls (cyber hygiene or standard practice) in NIST SP 800-53 R5 to mitigations as defined in ATT&CK for Enterprise and ATT&CK for ICS, as documented in [11].

The CSA Tool databases will be updated to reflect the reissued CNSSI 1253 [14], which updates controls[3] to reflect NIST SP 800-53 R5; the RMF baselines (now published as NIST SP 800-53A) will also be updated.

[3] For ease of exposition, the term "control" will be used to refer to control enhancements (e.g., AC-3(1)) as well as base controls (e.g., AC-3). In the RMF, selection of a control enhancement assumes the selection of its base control.

2 Analysis Process

This section describes the analysis process used to construct the tables mapping cyber resiliency controls and approaches to the CSEIG CSAs. The CSAs were analyzed one at a time, with ongoing cross checking to ensure consistency. This process is illustrated in general terms in Figure 2. The process is described in more detail below.

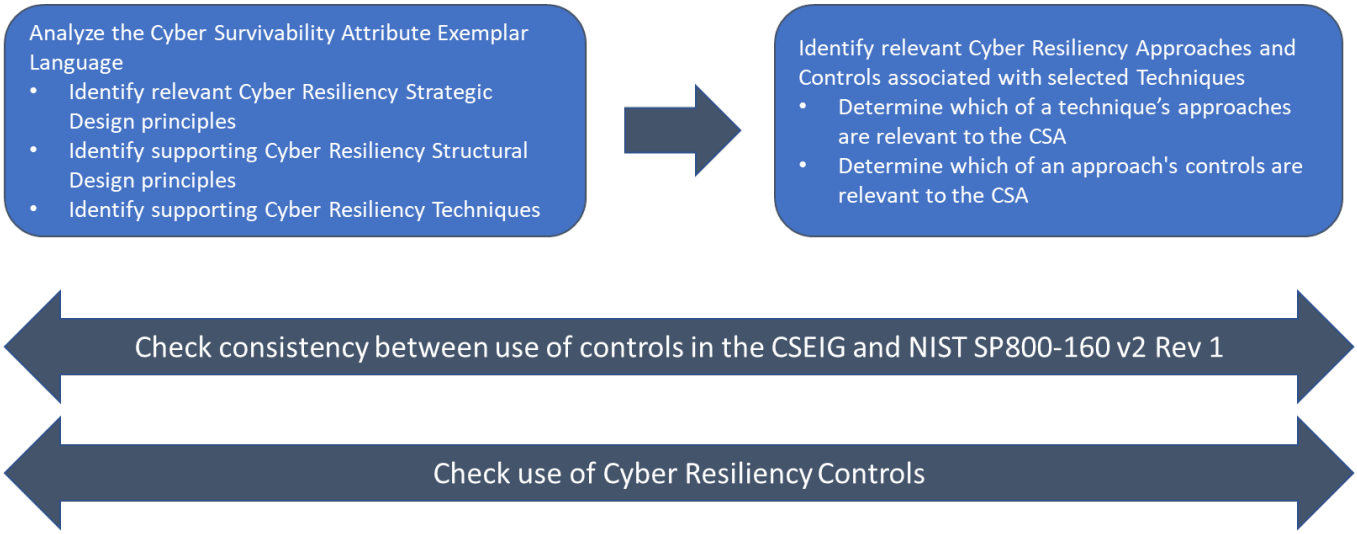

Figure 2. Overview of the Cyber Resiliency Analysis Process for CSA

2.1 Analyze CSA Exemplar Language

The blue box on the left in Figure 2 illustrates the prior analysis [7], which served as the starting point for the analysis described below. That prior analysis used four steps to determine which cyber resiliency techniques could support the effective implementation and demonstration of a CSA, based on analysis of the CSA exemplar language found in the Joint Chiefs of Staff, "Cyber Survivability Endorsement Implementation Guide, Version 3.0" [1] and "New DoD approaches on the Cyber Survivability of Weapon Systems" [10]:

1. Assess each CSA in the context of the cyber resiliency strategic design principles to determine which principles align with the CSA's aims as described in the CSA definition.
2. Select specific structural design principles associated with the strategic design principles. This selection is based on the CSA definitions, the CSA exemplar language, and Table D-10 in NIST SP 800-160 Vol. 2 R1 [6] which is reproduced in Appendix B as Table 15.
3. Identify the cyber resiliency techniques associated with the structural design principles for each CSA. Assess the selected techniques to determine if they can be used to support that CSA. This selection uses Table D-15 in NIST SP 800-160 Vol. 2 R1 [6] which is reproduced in Appendix B as Table 16.
4. Review the results of step three in light of the political, operational, economic, and technical (POET) considerations described in the MITRE document, "Cyber Resiliency Assessment: Enabling Architectural Improvement (MTR 120407, PR12-3795)," [15] determine the additional cyber resiliency techniques might be applied and what considerations apply.

At each step of this analysis, the exemplar language of the CSAs was used as the basis for selecting the cyber resiliency constructs.

2.2 Methodology

The blue box on the right in Figure 2 describes the analysis method used to produce the tables in this report. That analysis started with the cyber resiliency techniques identified for each CSA in [7] using the process described in 2.1 above and expanded them to include the cyber resiliency approaches and controls. While that prior analysis used the exemplar language in [10] and the initial version of NIST SP 800-160 Vol. 2 [5], the analysis presented in this report uses the exemplar language in the Joint Chiefs of Staff "Cyber Survivability Endorsement Implementation Guide, Version 3.0" [1], "Cyber Survivability for Future and Legacy DoD Weapon Systems" [2] and NIST SP 800-160 Vol. 2 R1 [6].

The analyses presented here started with the results of step 3 above and identified the cyber resiliency approaches and controls for each CSA based on the Table E-1 in 800-160 Vol. 2 R1 which is reproduced in Appendix C, Table 17. Each of the cyber resiliency approaches associated with a technique that was identified in step 3 above, was analyzed to determine if it could be used to support implementation of the CSA.

Next, the controls associated with the cyber resiliency approach were evaluated. In some cases, the selected controls were necessary to implement the type of resiliency identified. In other cases, the selected controls may be useful in implementing cyber resiliency depending on how the control is implemented and the specific implementation or environment.

At each step of this analysis the exemplar language of the CSAs was used as the basis for selecting the cyber resiliency constructs. While the identification of controls in the CSEIG for each CSA was used as a reference, it was not used as the determining factor since the purpose of this analysis was to look at how cyber resiliency could support the implementation of each CSA, and many of the cyber resiliency controls are outside of the baselines considered in the CSEIG identification.

This work was reviewed by an internal MITRE group focused on NIST SP 800-53 controls and an external group of cyber survivability subject matter experts (SMEs).

2.3 Limitations and Caveats

The restricted scope of the analysis presented in this report must be understood for its results to be used correctly. The following are a list of this report's limitations and caveats:

- *Based on analysis of exemplar language*. The mappings of cyber resiliency controls and approaches to CSAs presented in this report are based on engineering analysis of the exemplar language. The cyber resiliency controls mapped to a particular CSA are intended to serve as a starting point for a system-specific analysis. The CSEIG calls for CSAs for a system to be selected based on the system's Cyber Survivability Risk Category (CSRC); to be tailored from the exemplar language based on the system's mission requirements, operational environment, and threat environment; and to be refined over the system development lifecycle (SDLC). (See the Joint Chiefs of Staff "Cyber Survivability Endorsement Implementation Guide, Version 3.0" [1], Section 8.). Such tailoring and refinement can result in omitting some controls identified in the tables, as well as in identifying additional controls.

- *Restricted to cyber resiliency controls.* As noted in Section 1, non-cyber resiliency controls have also been identified for CSAs and included in the AFRL CSA Tool. However, the analysis in this report only considers cyber resiliency controls.
- *Does not include related controls.* This analysis does not consider related controls for the identified cyber resiliency controls.[4] This limitation prevents the analysis from daisy-chaining into including a large percentage of NIST SP 800-53 R5 controls, with no contribution to an engineering understanding of how related controls support CSAs.
- *Assumed use of controls*. The inclusion of a control in a system's requirements does not in itself guarantee a more effective implementation of a CSA. The amount of support provided by a cyber resiliency control depends on (i) how the control is specified (e.g., via Assignment statements or Selections), (ii) how the control is implemented, and (iii) how the implementation is used. Thus, while the mapping tables in Section 3 rely on the descriptions of the controls in NIST SP 800-53 R5 (including not only the wording of the control, but also the Supplemental Guidance) and the CSA exemplar language, the effectiveness of a control in supporting a CSA (like the CSA itself) will depend on the context in which the controls are applied, and the CSA is implemented.
- *Represents varying degrees of support*. While the cyber resiliency constructs identified for a given CSA all support the implementation of that CSA, the degree to which they support that CSA was not analyzed.
- *Intended to be down selected*. The controls listed in the tables are a starting point. The selection of cyber resiliency constructs, particularly controls, for a CSA must be tailored based on an engineering analysis. As noted in NIST SP 800-160 Vol. 2 R1 [6], some cyber resiliency techniques (and hence approaches and controls) may be incompatible with each other.
- *Limited to required techniques.* Some techniques are required by a structural design principle, while other techniques are typically used in conjunction with required techniques to apply the design principle more effectively, depending on the type of system to which the principle is applied. With one exception, only the required techniques were considered in creating the mappings. The exception is the use of the Obfuscation approach within the Deception technique to support the *Control visibility and use* structural design principle.
- *Based on non-CUI information about the CSEIG, which continues to evolve*. The analysis is based on three unclassified sources, which do not have the Controlled Unclassified Information (CUI) restriction: the Joint Chief of Staff's "Cyber Survivability Endorsement Implementation Guide, Version 3.0" [1], "Cyber Survivability for Future and Legacy DoD Weapon Systems" [2], and "New DoD approaches on the Cyber Survivability of Weapon Systems" [10]. A more detailed analysis could be based on other

[4] Controls can be *related* in two ways. First, there is an assumed dependency of a control enhancement on its base control: NIST SP 800-53 states that "The selection and implementation of control enhancements *always* requires the selection and implementation of the base control." Second, for many controls NIST SP 800-53 identifies one or more related controls. These are controls "that impact or support the implementation of a particular control or control enhancement, address a related security or privacy capability, or are referenced in the discussion [...] When a control is designated as a related control, a corresponding designation is made on that control in its source location in the catalog to illustrate the two-way relationship." Because a control enhancement is inherently related to its base control, that base control is not listed under the enhancement's related controls.

volumes of the CSEIG. In addition, the CSEIG continues to evolve. Therefore, this analysis should be revisited as updates to the CSEIG are published.

3 Mapping Tables

This section provides the tables mapping cyber resiliency design principles, techniques, approaches, and controls to the CSAs. One table is provided for each CSA. As noted in Section 2.3, the potential efficacy of a control in supporting a CSA depends on (i) how the control is specified (e.g., via Assignment statements or Selections), (ii) how the control is implemented, and (iii) how the implementation is used. The system, environment, mission, and organization in which the control is applied will impact these factors.

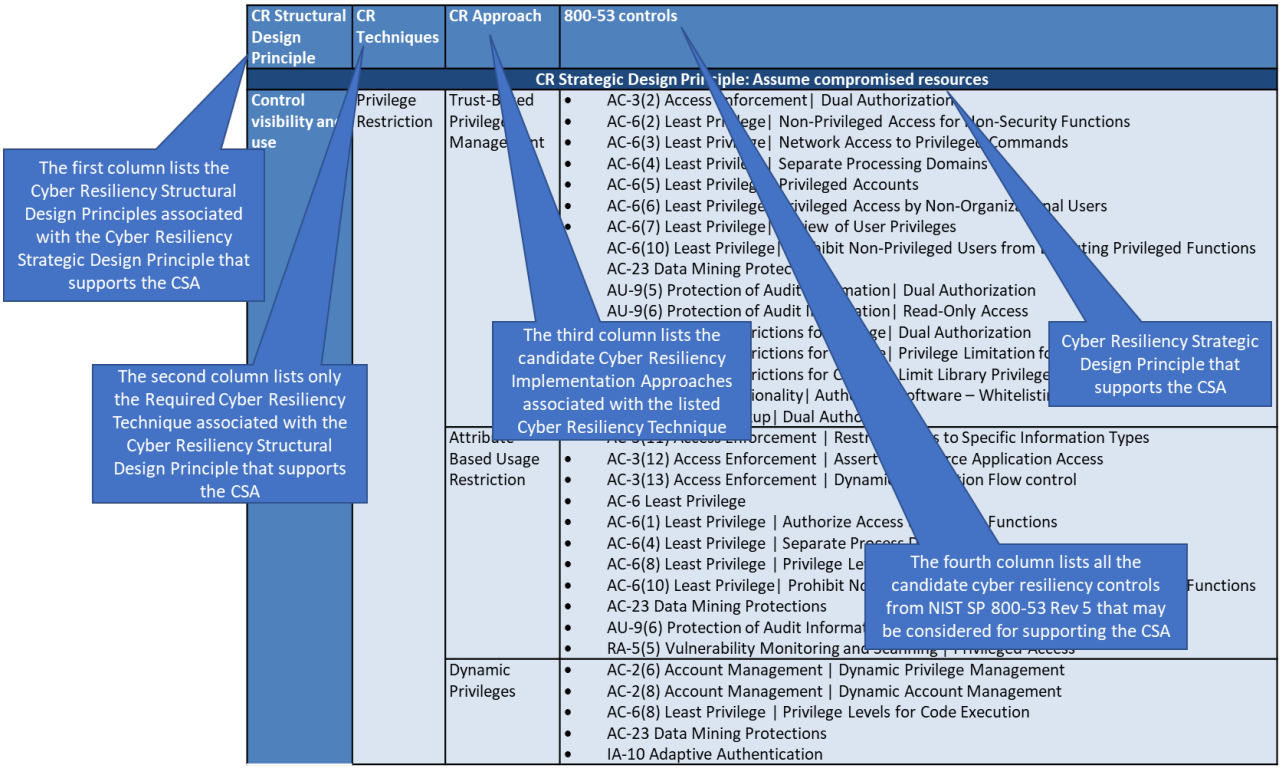

Figure 3. How to Read the CSA Tables

Figure 3 describes how the entries in the tables should be interpreted. There may be multiple cyber resiliency strategic design principles that support an individual CSA. These are in the dark blue cell(s) of the tables.

3.1 CSA-01

CSA 01 – **Control Access**: System shall only allow identified, authenticated, and authorized persons and non-person entities (including all assigned cyber defenders and their tools) access or interconnection to system or sub-system elements. The capability shall enforce a validation mechanism to protect the C, I, A [confidentiality, integrity, and availability] of system resources (e.g., memory, files, interfaces, logical networks). The system shall employ anti-tamper measures that include features for protection of critical system components, information technologies, and maintenance of technology/program protection. Physical access to the system shall also be controlled. [1], [2]

Table 2. Cyber Resiliency Constructs Supporting CSA-01

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
CR Strategic Design Principle: Assume compromised resources			
Control visibility and use	Privilege Restriction	Trust-Based Privilege Management	• AC-3(2) Access Enforcement| Dual Authorization • AC-6(2) Least Privilege| Non-Privileged Access for Non-Security Functions • AC-6(3) Least Privilege| Network Access to Privileged Commands • AC-6(4) Least Privilege| Separate Processing Domains • AC-6(5) Least Privilege| Privileged Accounts • AC-6(6) Least Privilege| Privileged Access by Non-Organizational Users • AC-6(7) Least Privilege| Review of User Privileges • AC-6(10) Least Privilege| Prohibit Non-Privileged Users from Executing Privileged Functions • AC-23 Data Mining Protection • AU-9(5) Protection of Audit Information| Dual Authorization • AU-9(6) Protection of Audit Information| Read-Only Access • CM-5(4) Access Restrictions for Change| Dual Authorization • CM-5(5) Access Restrictions for Change| Privilege Limitation for Production and Operation • CM-5(6) Access Restrictions for Change| Limit Library Privileges • CM-7(5) Least Functionality| Authorized Software – Whitelisting • CP-9(7) System Backup| Dual Authorization
		Attribute-Based Usage Restriction	• AC-3(11) Access Enforcement | Restrict Access to Specific Information Types • AC-3(12) Access Enforcement | Assert and Enforce Application Access • AC-3(13) Access Enforcement | Dynamic Information Flow control • AC-6 Least Privilege • AC-6(1) Least Privilege | Authorize Access to Security Functions • AC-6(4) Least Privilege | Separate Process Domains • AC-6(8) Least Privilege | Privilege Levels for Code Execution • AC-6(10) Least Privilege| Prohibit Non-Privileged Users from Executing Privileged Functions • AC-23 Data Mining Protection • AU-9(6) Protection of Audit Information| Read-Only Access • RA-5(5) Vulnerability Monitoring and Scanning | Privileged Access
		Dynamic Privileges	• AC-2(6) Account Management | Dynamic Privilege Management • AC-2(8) Account Management | Dynamic Account Management • AC-6(8) Least Privilege | Privilege Levels for Code Execution • AC-23 Data Mining Protection • IA-10 Adaptive Authentication
	Segmentation	Predefined Segmentation	• AC-4(2) Information Flow Enforcement | Processing Domains • AC-4(21) Information Flow Enforcement | Physical or Logical Separation of Information Flows • AC-6(4) Least Privilege| Separate Processing Domains • AU-6(8) Audit Record Review, Analysis, and Reporting | Full Text Analysis of Privileged Commands • AU-9(2) Protection of Audit Information | Store on Separate Physical Systems and Components • CM-4(1) Impact Analyses | Separate Test Environments • CM-7(5) Least Functionality | Authorized Software • IA-2(13) Identification and Authentication | Out-Of-Band Authentication • IR-4(12) Incident Handling | Malicious Code and Forensic Analysis

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
			• MA-4(4) Nonlocal Maintenance | Authentication and Separation of Maintenance Sessions • SC-2 Separation of System and User Functionality • SC-2(1) Separation of System and User Functionality | Interfaces for Non-Privileged Users • SC-3 Security Function Isolation • SC-3(1) Security Function Isolation | Hardware Separation • SC-3(2) Security Function Isolation | Access and Flow Control Functions • SC-3(5) Security Function Isolation | Layered Structures • SC-7 Boundary Protection • SC-7(13) Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components • SC-7(15) Boundary Protection | Network Privileged Accesses • SC-7(21) Boundary Protection | Isolation of System Components • SC-7(22) Boundary Protection | Separate Subnets for Connecting to Different Security Domains • SC-8(5) Transmission Confidentiality and Integrity | Protected Distribution System • SC-11 Trusted Path • SC-32 System Partitioning • SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions • SC-39 Process Isolation • SC-39(1) Process Isolation | Hardware Separation • SC-39(2) Process Isolation | Separation Execution Domains Per Thread • SC-44 Detonation Chambers • SC-49 Hardware-Enforced Separation and Policy Enforcement • SC-50 Software-Enforced Separation and Policy Enforcement
		Dynamic Segmentation and Isolation	• CM-7(5) Least Functionality | Authorized Software • SC-7(20) Boundary Protection | Dynamic Isolation and Segregation • SC-18(5) Mobile Code | Allow Execution Only in Confined Environments • SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions • SC-35 External Malicious Code Identification • SC-39 Process Isolation • SC-39(1) Process Isolation | Hardware Separation • SC-39(2) Process Isolation | Separation Execution Domains Per Thread
Determine ongoing trustworthiness	Substantiated Integrity	Integrity Checks	• AC-4(8) Information Flow Enforcement | Security and Privacy Policy Filters • AC-4(12) Information Flow Enforcement | Data Type Identifiers • AU-9(1) Protection of Audit Information | Hardware Write-Once Media • AU-9(3) Protection of Audit Information | Cryptographic Protection • AU-9(6) Protection of Audit Information | Read-Only Access • CM-14 Signed Components • IA-3(1) Device Identification and Authentication | Cryptographic Bidirectional Authentication • PE-3(5) Physical Access Control | Tamper Protection • SC-8(1) Transmission Confidentiality and Integrity | Cryptographic Protection

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
			• SC-8(5) Transmission Confidentiality and Integrity | Protected Distribution System • SC-28(1) Protection of Information at Rest | Cryptographic Protection • SC-34 Non-Modifiable Executable Programs • SC-34(2) Non-Modifiable Executable Programs | Integrity Protection on Read-Only Media • SC-51 Hardware-Based Protection • SI-6 Security and Privacy Function Verification • SI-7 Software, Firmware, and Information Integrity • SI-7(1) Software, Firmware, and Information Integrity | Integrity Checks • SI-7(5) Software, Firmware, and Information Integrity | Automated Response to Integrity Violations • SI-7(6) Software, Firmware, and Information Integrity | Cryptographic Protection • SI-7(7) Software, Firmware, and Information Integrity | Integration of Detection and Response • SI-7(9) Software, Firmware, and Information Integrity | Verify Boot Process • SI-7(10) Software, Firmware, and Information Integrity | Protection of Boot Firmware • SI-7(12) Software, Firmware, and Information Integrity | Integrity Verification • SI-15 Information Output Filtering • SR-4(3) Provenance | Validate as Genuine and Not Altered • SR-9 Tamper Resistance and Detection • SR-9(1) Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle
		Behavior Validation	• AC-2(12) Account Management | Account Monitoring for Atypical Usage • AU- 6 Audit Record Review, Analysis, and Reporting • IR-4(13) Incident Handling | Behavior Analysis • SC-36(1) Distributed Processing and Storage | Polling Techniques • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis • SI-4(4) System Monitoring | Inbound and Outbound Communications Traffic • SI-4(13) System Monitoring | Analyze Traffic and Event Patterns • SI-10(3) Information Input Validation |Predictable Behavior • SR-10 Inspection of Systems or Components • SR-11 Component Authenticity

3.2 CSA-02

CSA 02 – **Reduce System's Cyber Detectability**: System survivability requires that signaling and communications (both wired and wireless) implemented by the system (or state "supported by system/capability") shall minimize the ability of an adversary to monitor and/or target system and/or supported DoD weapon systems through its emanations, which may include deception. [1], [2], and [10]

Table 3. Cyber Resiliency Constructs Supporting CSA-02

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
	CR Strategic Design Principle: Reduce attack surfaces		
Control visibility and use	Segmentation	Predefined Segmentation	• AC-4(2) Information Flow Enforcement | Processing Domains • AC-4(21) Information Flow Enforcement | Physical or Logical Separation of Information Flows • AC-6(4) Least Privilege| Separate Processing Domains • AU-9(2) Protection of Audit Information | Store on Separate Physical Systems and Components • CM-4(1) Impact Analyses | Separate Test Environments • SC-2 Separation of System and User Functionality • SC-2(1) Separation of System and User Functionality | Interfaces for Non-Privileged Users • SC-3 Security Function Isolation • SC-3(1) Security Function Isolation | Hardware Separation • SC-3(2) Security Function Isolation | Access and Flow Control Functions • SC-3(5) Security Function Isolation | Layered Structures • SC-7 Boundary Protection • SC-7(13) Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components • SC-7(15) Boundary Protection | Network Privileged Accesses • SC-7(21) Boundary Protection | Isolation of System Components • SC-7(22) Boundary Protection | Separate Subnets for Connecting to Different Security Domains • SC-32 System Partitioning • SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions • SC-39 Process Isolation • SC-39(1) Process Isolation | Hardware Separation • SC-39(2) Process Isolation | Separation Execution Domains Per Thread • SC-44 Detonation Chambers • SC-49 Hardware-Enforced Separation and Policy Enforcement • SC-50 Software-Enforced Separation and Policy Enforcement
		Dynamic Segmentation and Isolation	• SC-7(20) Boundary Protection | Dynamic Isolation and Segregation • SC-18(5) Mobile Code | Allow Execution Only in Confined Environments • SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions • SC-39 Process Isolation • SC-39(1) Process Isolation | Hardware Separation • SC-39(2) Process Isolation | Separation Execution Domains Per Thread
	Deception	Obfuscation	• CP-9(8) System Backup | Cryptographic Protection • SC-7(16) Boundary Protection | Prevent Discovery of System Components • SC-8(4) Transmission Confidentiality and Integrity | Conceal or Randomize Communications • SC-30 Concealment and Misdirection • SC-30(5) Concealment and Misdirection | Concealment of System Components • SC-40(2) Wireless Link Protection | Reduce Detection Potential • SC-40(3) Wireless Link Protection | Imitative or Manipulative Communications Deception • SR-3(2) Supply Chain Controls and Processes | Limitation of Harm

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
			• SR-5 Acquisition Strategies, Tools, And Methods • SR-9(1) Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle
Maximize transience	Non-Persistence	Non-Persistent Information	• SC-25 Thin Nodes • SI-21 Information Refresh
		Non-Persistent Services	• AC-23 Data Mining Protection • SC-25 Thin Nodes • SI-14 Non-Persistence • SI-14(1) Non-Persistence | Refresh from Trusted Sources
		Non-Persistent Connectivity	• SC-10 Network Disconnect • SC-15(1) Collaborative Computing Devices | Physical or Logical Disconnect • SI-14(3) Non-Persistence | Non-Persistent Connectivity
	Unpredictability	Temporal Unpredictability	• SC-30(2) Concealment and Misdirection | Randomness • SC-30(3) Concealment and Misdirection | Change Processing and Storage Locations • SC-40(3) Wireless Link Protection | Imitative or Manipulative Communications Deception
		Contextual Unpredictability	• SC-8(4) Transmission Confidentiality and Integrity | Conceal or Randomize Communications • SC-30(2) Concealment and Misdirection | Randomness • SC-40(3) Wireless Link Protection | Imitative or Manipulative Communications Deception
CR Strategic Design Principle: Support agility and architect for adaptability			
Make resources location-versatile	Dynamic Positioning	Functional Relocation of Sensors	• IR-4(2) Incident Handling | Dynamic Reconfiguration
		Functional Relocation of Cyber Resources	• SC-7(16) Boundary Protection | Prevent Discovery of System Components • SC-30(3) Concealment and Misdirection | Change Processing and Storage Locations • SC-36 Distributed Processing and Storage
		Asset Mobility	• SC-36 Distributed Processing and Storage
		Fragmentation	• SI-23 Information Fragmentation
		Distributed Functionality	• SC-36 Distributed Processing and Storage
	Unpredictability	Temporal Unpredictability	• SC-30(2) Concealment and Misdirection | Randomness • SC-30(3) Concealment and Misdirection | Change Processing and Storage Locations • SC-40(3) Wireless Link Protection | Imitative or Manipulative Communications Deception
		Contextual Unpredictability	• SC-8(4) Transmission Confidentiality and Integrity | Conceal or Randomize Communications • SC-30(2) Concealment and Misdirection | Randomness • SC-40(3) Wireless Link Protection | Imitative or Manipulative Communications Deception

3.3 CSA-03

CSA-03 – **Secure Transmissions and Communications**: System shall ensure all transmissions and communications of data 'in transit' are protected commensurate with its confidentiality and integrity requirements. System shall only use NSA-certified cryptographic devices. [1] [2]

[10] adds: System shall prevent unauthorized transmissions and communications, including attempted data exfiltration, from the system to an unauthorized person or non-person entity.

Table 4. Cyber Resiliency Constructs Supporting CSA-03

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
CR Strategic Design Principle: Focus on common critical assets			
Layer defenses and partition resources	Coordinated Protection	Calibrated Defense-in-Depth	• IA-2(6) Identification and Authentication | Access to Accounts - Separate Device • IA-2(13) Identification and Authentication | Out-Of-Band Authentication
		Orchestration	• IA-2(6) Identification and Authentication | Access to Accounts - Separate Device • IA-2(13) Identification and Authentication | Out-Of-Band Authentication • PE-6(2) Monitoring Physical Access | Automated Intrusion Recognition and Responses
	Segmentation	Predefined Segmentation	• AC-4(2) Information Flow Enforcement | Processing Domains • AC-4(21) Information Flow Enforcement | Physical or Logical Separation of Information Flows • IA-2(13) Identification and Authentication | Out-Of-Band Authentication • MA-4(4) Nonlocal Maintenance | Authentication and Separation of Maintenance Sessions • SC-3(2) Security Function Isolation | Access and Flow Control Functions • SC-7 Boundary Protection • SC-7(15) Boundary Protection | Network Privileged Accesses • SC-8(5) Transmission Confidentiality and Integrity | Protected Distribution System • SC-11 Trusted Path
Maintain Redundancy	Redundancy	Surplus Capacity	• SC-5(2) Denial of Service Protection | Capacity, Bandwidth, and Redundancy
		Replication	• PE-9(1) Power Equipment and Cabling | Redundant Cabling
Determine ongoing trustworthiness	Substantiated Integrity	Integrity Checks	• IA-3(1) Device Identification and Authentication | Cryptographic Bidirectional Authentication • PE-3(5) Physical Access Control | Tamper Protection • SC-8(1) Transmission Confidentiality and Integrity | Cryptographic Protection • SC-8(5) Transmission Confidentiality and Integrity | Protected Distribution System • SR-9 Tamper Resistance and Detection
		Provenance Tracking	• SC-7(11) Boundary Protection | Restrict Incoming Communications Traffic • SC-11 Trusted Path • SI-10(5) Information Input Validation | Restrict Inputs to Trusted Sources and Approved Formats
		Behavior Validation	• SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis • SI-4(4) System Monitoring | Inbound and Outbound Communications Traffic • SI-4(13) System Monitoring | Analyze Traffic and Event Patterns
Limit the need for trust	Realignment	Offloading	• SC-7(15) Boundary Protection | Network Privileged Accesses

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
Maximize transience	Non-Persistence	Non-Persistent Connectivity	• SC-7(10) Boundary Protection | Prevent Exfiltration • SC-10 Network Disconnect • SC-15(1) Collaborative Computing Devices | Physical or Logical Disconnect • SI-14(3) Non-Persistence | Non-Persistent Connectivity
		Non-Persistent Services	• AC-12 Session Termination
CR Strategic Design Principle: Assume compromised resources			
Change or disrupt the attack surface	Dynamic Positioning	Functional Relocation of Cyber Resources	• SC-7(16) Boundary Protection | Prevent Discovery of System Components • SC-30(3) Concealment and Misdirection | Change Processing and Storage Locations • SC-36 Distributed Processing and Storage
		Asset Mobility	• SC-36 Distributed Processing and Storage
		Distributed Functionality	• SC-36 Distributed Processing and Storage
	Non-Persistence	Non-Persistent Connectivity	• SC-7(10) Boundary Protection | Prevent Exfiltration • SC-10 Network Disconnect • SC-15(1) Collaborative Computing Devices | Physical or Logical Disconnect • SI-14(3) Non-Persistence | Non-Persistent Connectivity
		Non-Persistent Services	• AC-12 Session Termination
Limit the need for trust	Privilege Restriction	Trust-Based Privilege Management	• AC-6(3) Least Privilege| Network Access to Privileged Commands
	Realignment	Offloading	• SC-7(15) Boundary Protection | Network Privileged Accesses
Control visibility and use	Privilege Restriction	Trust-Based Privilege Management	• AC-3(2) Access Enforcement| Dual Authorization • AC-6(3) Least Privilege| Network Access to Privileged Commands • AC-6(5) Least Privilege| Privileged Accounts • AC-6(6) Least Privilege| Privileged Access by Non-Organizational Users • AC-6(10) Least Privilege| Prohibit Non-Privileged Users from Executing Privileged Functions • AC-23 Data Mining Protection • AU-9(5) Protection of Audit Information| Dual Authorization • CM-5(4) Access Restrictions for Change| Dual Authorization • CM-5(5) Access Restrictions for Change| Privilege Limitation for Production and Operation • CM-5(6) Access Restrictions for Change| Limit Library Privileges • CP-9(7) System Backup| Dual Authorization
		Attribute-Based Usage Restriction	• AC-3(11) Access Enforcement | Restrict Access to Specific Information Types • AC-3(12) Access Enforcement | Assert and Enforce Application Access • AC-3(13) Access Enforcement | Dynamic Information Flow control • AC-6 Least Privilege • AC-6(1) Least Privilege | Authorize Access to Security Functions • AC-6(10) Least Privilege| Prohibit Non-Privileged Users from Executing Privileged Functions • AU-9(6) Protection of Audit Information| Read-Only Access • RA-5(5) Vulnerability Monitoring and Scanning | Privileged Access

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
		Dynamic Privileges	• AC-2(6) Account Management | Dynamic Privilege Management • AC-2(8) Account Management | Dynamic Account Management
	Segmentation	Predefined Segmentation	• AC-4(2) Information Flow Enforcement | Processing Domains • AC-4(21) Information Flow Enforcement | Physical or Logical Separation of Information Flows • IA-2(13) Identification and Authentication | Out-Of-Band Authentication • MA-4(4) Nonlocal Maintenance | Authentication and Separation of Maintenance Sessions • SC-3(2) Security Function Isolation | Access and Flow Control Functions • SC-7 Boundary Protection • SC-7(15) Boundary Protection | Network Privileged Accesses • SC-8(5) Transmission Confidentiality and Integrity | Protected Distribution System • SC-11 Trusted Path
	Deception	Obfuscation	• IA-3(1) Device Identification and Authentication | Cryptographic Bidirectional Authentication • SC-8(4) Transmission Confidentiality and Integrity | Conceal or Randomize Communications • SC-40(2) Wireless Link Protection | Reduce Detection Potential • SC-40(3) Wireless Link Protection | Imitative or Manipulative Communications Deception

3.4 CSA-04

CSA-04 – **Protect System's Information from Exploitation**: System shall ensure all data 'at rest' is protected commensurate with its confidentiality and integrity requirements. System shall prevent unauthorized access, use, modification, and transfer/removal of data, including attempted exfiltration, from the system to unauthorized person and non-person entities throughout the system's lifecycle (including development). [1], [2]

Note that [10] did not mention integrity requirements. Note also that Deception supports, but is not required for, Control Visibility and Use and Change and Disrupt Attack Surfaces. One Deception approach that should be considered for CSA-04 is Disinformation with control SC-30(4) Concealment and Misdirection | Misleading Information.

Table 5. Cyber Resiliency Constructs Supporting CSA-04

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
CR Strategic Design Principle: Focus on common critical assets			
Contain and exclude behaviors	Privilege Restriction	Trust-Based Privilege Management	• AC-23 Data Mining Protection • AU-9(5) Protection of Audit Information| Dual Authorization • AU-9(6) Protection of Audit Information| Read-Only Access
		Attribute-Based Usage Restriction	• AC-3(11) Access Enforcement | Restrict Access to Specific Information Types • AC-23 Data Mining Protection • AU-9(6) Protection of Audit Information| Read-Only Access
		Dynamic Privileges	• AC-23 Data Mining Protection

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
	Segmentation	Predefined Segmentation	• AC-4(2) Information Flow Enforcement | Processing Domains • AC-4(21) Information Flow Enforcement | Physical or Logical Separation of Information Flows • AU-9(2) Protection of Audit Information | Store on Separate Physical Systems and Components • SC-8(5) Transmission Confidentiality and Integrity | Protected Distribution System
Layer defenses and partition resources	Coordinated Protection	Self-Challenge	• SC-7(10) Boundary Protection | Prevent Exfiltration
	Segmentation	Predefined Segmentation	• AC-4(2) Information Flow Enforcement | Processing Domains • AC-4(21) Information Flow Enforcement | Physical or Logical Separation of Information Flows • AU-9(2) Protection of Audit Information | Store on Separate Physical Systems and Components • SC-8(5) Transmission Confidentiality and Integrity | Protected Distribution System
Maximize transience	Non-Persistence	Non-Persistent Information	• SC-7(10) Boundary Protection | Prevent Exfiltration • SC-25 Thin Nodes • SC-34(1) Non-Modifiable Executable Programs | No Writable Storage • SI-14(1) Non-Persistence | Refresh from Trusted Sources • SI-14(2) Non-Persistence | Non-Persistent Information • SI-21 Information Refresh
Determine ongoing trustworthiness	Substantiated Integrity	Integrity Checks	• AC-4(8) Information Flow Enforcement | Security and Privacy Policy Filters • AC-4(12) Information Flow Enforcement | Data Type Identifiers • AU-9(1) Protection of Audit Information | Hardware Write-Once Media • AU-9(3) Protection of Audit Information | Cryptographic Protection • AU-9(6) Protection of Audit Information | Read-Only Access • SC-8(1) Transmission Confidentiality and Integrity | Cryptographic Protection • SC-8(5) Transmission Confidentiality and Integrity | Protected Distribution System • SC-28(1) Protection of Information at Rest | Cryptographic Protection • SI-7 Software, Firmware, and Information Integrity • SI-7(1) Software, Firmware, and Information Integrity | Integrity Checks • SI-7(5) Software, Firmware, and Information Integrity | Automated Response to Integrity Violations • SI-7(6) Software, Firmware, and Information Integrity | Cryptographic Protection
Change or disrupt the attack surface	Dynamic Positioning	Functional Relocation of Cyber Resources	• SC-36 Distributed Processing and Storage
		Asset Mobility	• SC-36 Distributed Processing and Storage
		Fragmentation	• SI-23 Information Fragmentation
		Distributed Functionality	• SC-36 Distributed Processing and Storage

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
	Non-Persistence	Non-Persistent Information	• SC-7(10) Boundary Protection | Prevent Exfiltration • SC-25 Thin Nodes • SC-34(1) Non-Modifiable Executable Programs | No Writable Storage • SI-14(1) Non-Persistence | Refresh from Trusted Sources • SI-14(2) Non-Persistence | Non-Persistent Information • SI-21 Information Refresh
Control visibility and use	Privilege Restriction	Trust-Based Privilege Management	• AC-23 Data Mining Protection • AU-9(5) Protection of Audit Information| Dual Authorization • AU-9(6) Protection of Audit Information| Read-Only Access
		Attribute-Based Usage Restriction	• AC-3(11) Access Enforcement | Restrict Access to Specific Information Types • AC-23 Data Mining Protection • AU-9(6) Protection of Audit Information| Read-Only Access
		Dynamic Privileges	• AC-23 Data Mining Protection
	Segmentation	Predefined Segmentation	• AC-4(2) Information Flow Enforcement | Processing Domains • AC-4(21) Information Flow Enforcement | Physical or Logical Separation of Information Flows • AU-9(2) Protection of Audit Information | Store on Separate Physical Systems and Components • SC-8(5) Transmission Confidentiality and Integrity | Protected Distribution System
	Deception	Disinformation	• SC-30(4) Concealment and Misdirection | Misleading Information
		Obfuscation	• CP-9(8) System Backup | Cryptographic Protection • SC-8(4) Transmission Confidentiality and Integrity | Conceal or Randomize Communications • SC-28(1) Protection of Information at Rest | Cryptographic Protection

3.5 CSA-05

CSA-05 – **Partition and Ensure Critical Functions at Mission Completion Performance Levels**: System partitioning shall implement technical/logical mitigations including logical and physical segmentation. The system shall be able to maintain mission critical functions at minimum performance thresholds identified within the system's CONOPS [Concept of Operations]. Compromise of non-critical functions shall not significantly impact system mission capability. [1], [2], and [10]

Table 6. Cyber Resiliency Constructs Supporting CSA-05

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
CR Strategic Design Principle: Focus on common critical assets			
Plan and manage diversity	Diversity	Architectural Diversity	• AU-9(7) Protection of Audit Information | Store on Component with Different Operating System • CP-8(3) Telecommunications Services | Separation of Primary and Alternate Providers • CP-11 Alternate Communications Protocols • CP-13 Alternative Security Mechanisms • SC-29 Heterogeneity

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
			• SC-29(1) Heterogeneity | Virtualization Techniques
		Design Diversity	• CP-11 Alternate Communications Protocols • CP-13 Alternative Security Mechanisms • SA-17(9) Developer Security Architecture and Design | Design Diversity
		Synthetic Diversity	• SI-16 Memory Protection
		Path Diversity	• AC-7(4) Unsuccessful Logon Attempts | Use of Alternate Authentication Factor • IA-2(6) Identification and Authentication | Access to Accounts - Separate Device • IA-2(13) Identification and Authentication | Out-Of-Band Authentication • SC-37 Out-Of-Band Channels • SC-47 Alternate Communication Paths
Maintain redundancy	Redundancy	Protected Backup and Restore	• CP-9 System Backup • CP-9(8) System Backup | Cryptographic Protection
		Surplus Capacity	• SC-5(2) Denial of Service Protection | Capacity, Bandwidth, and Redundancy
		Replication	• CP-9(6) System Backup | Redundant Secondary System • PE-9(1) Power Equipment and Cabling | Redundant Cabling • PE-11(1) Emergency Power | Alternate Power Supply – Minimal Operational Capability • PE-11(2) Emergency Power | Alternate Power Supply – Self-Contained • PE-17 Alternate Work Site • SC-36 Distributed Processing and Storage
Manage resources (risk-) adaptively	Adaptive Response	Dynamic Reconfiguration	• AC-2(6) Account Management | Dynamic Privilege Management • AC-2(8) Account Management | Dynamic Account Management • AC-4(3) Information Flow Enforcement | Dynamic Information Flow Control • CP-2(5) Contingency Plan | Continue Missions and Business Functions • IR-4(2) Incident Handling | Dynamic Reconfiguration • IR-4(3) Incident Handling | Continuity of Operations • IR-4(9) Incident Handling | Dynamic Response Capability • IR-4(11) Incident Handling | Integrated Incident Response Team • SC-7(20) Boundary Protection | Dynamic Isolation and Segregation
		Dynamic Resource Allocation	• AC-2(8) Account Management | Dynamic Account Management • SC-5(2) Denial of Service Protection | Capacity, Bandwidth, and Redundancy
		Adaptive Management	• AC-2(8) Account Management | Dynamic Account Management • AC-4(3) Information Flow Enforcement | Dynamic Information Flow Control • CP-2(5) Contingency Plan | Continue Missions and Business Functions • CP-12 Safe Mode • CP-13 Alternative Security Mechanisms • IA-10 Adaptive Authentication

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
			• IR-4(3) Incident Handling | Continuity of Operations • IR-4(11) Incident Handling | Integrated Incident Response Team • RA-3(3) Risk Assessment | Dynamic Threat Awareness • SI-4(3) System Monitoring | Automated Tool and Mechanism Integration • SI-4(7) System Monitoring | Automated Response to Suspicious Events • SI-7(5) Software, Firmware, and Information Integrity | Automated Response to Integrity Violations
Leverage health and status data	Analytic Monitoring	Sensor Fusion and Analysis	• AU-6(5) Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records • AU-6(6) Audit Record Review, Analysis, and Reporting | Correlation with Physical Monitoring • AU-6(9) Audit Record Review, Analysis, And Reporting | Correlation with Information from Nontechnical Sources • IR-4(4) Incident Handling | Information Correlation • RA-5(10) Vulnerability Monitoring and Scanning | Correlate Scanning Information • SI-4(3) System Monitoring | Automated Tool and Mechanism Integration • SI-4(24) System Monitoring | Indicators of Compromise
	Contextual Awareness	Dynamic Resource Awareness	• CA-7(3) Continuous Monitoring | Trend Analyses
		Dynamic Threat Awareness	• CA-7(3) Continuous Monitoring | Trend Analyses • PM-16(1) Threat Awareness Program | Automated Means for Sharing Threat Intelligence • RA-3(3) Risk Assessment | Dynamic Threat Awareness • RA-10 Threat Hunting
		Mission Dependency and Status Visualization	• CP-2(8) Contingency Plan | Identify Critical Assets • RA-9 Criticality Analysis • SI-4(1) System Monitoring | System-Wide Intrusion Detection System • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis
Maximize transience	Non-Persistence	Non-Persistent Services	• SC-25 Thin Nodes • SC-29(1) Heterogeneity | Virtualization Techniques • SI-14 Non-Persistence • SI-14(1) Non-Persistence | Refresh from Trusted Sources
		Non-Persistent Connectivity	• SC-7(10) Boundary Protection | Prevent Exfiltration • SC-10 Network Disconnect • SC-15(1) Collaborative Computing Devices | Physical or Logical Disconnect • SI-14(3) Non-Persistence | Non-Persistent Connectivity
CR Strategic Design Principle: Assume compromised resources			
Change or disrupt the attack surface	Dynamic Positioning	Functional Relocation of Cyber Resources	• SC-7(16) Boundary Protection | Prevent Discovery of System Components • SC-30(3) Concealment and Misdirection | Change Processing and Storage Locations • SC-36 Distributed Processing and Storage
		Asset Mobility	• SC-36 Distributed Processing and Storage
		Distributed Functionality	• SC-36 Distributed Processing and Storage

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
	Non-Persistence	Non-Persistent Services	• SC-25 Thin Nodes • SC-29(1) Heterogeneity | Virtualization Techniques • SI-14 Non-Persistence • SI-14(1) Non-Persistence | Refresh from Trusted Sources
		Non-Persistent Connectivity	• SC-7(10) Boundary Protection | Prevent Exfiltration • SC-10 Network Disconnect • SC-15(1) Collaborative Computing Devices | Physical or Logical Disconnect • SI-14(3) Non-Persistence | Non-Persistent Connectivity
Limit the need for trust	Coordinated Protection	Calibrated Defense-in-Depth	• IA-2(6) Identification and Authentication | Access to Accounts - Separate Device • IA-2(13) Identification and Authentication | Out-Of-Band Authentication • IA-10 Adaptive Authentication • PL-8(1) Security and Privacy Architecture | Defense in Depth
		Orchestration	• CP-2(5) Contingency Plan | Continue Missions and Business Functions • IA-2(6) Identification and Authentication | Access to Accounts - Separate Device • IA-2(13) Identification and Authentication | Out-Of-Band Authentication • IR-4(3) Incident Handling | Continuity of Operations • IR-4(11) Incident Handling | Integrated Incident Response Team • SA-17(8) Developer Security Architecture and Design | Orchestration • SC-3(5) Security Function Isolation | Layered Structures
	Realignment	Offloading	• PM-7(1) Enterprise Architecture | Offloading • RA-9 Criticality Analysis • SC-3(5) Security Function Isolation | Layered Structures • SC-7(15) Boundary Protection | Network Privileged Accesses • SC-25 Thin Nodes
		Restriction	• SC-3(3) Security Function Isolation | Minimize Nonsecurity Functionality
Maximize transience	Non-Persistence	Non-Persistent Services	• SC-25 Thin Nodes • SC-29(1) Heterogeneity | Virtualization Techniques • SI-14 Non-Persistence • SI-14(1) Non-Persistence | Refresh from Trusted Sources
		Non-Persistent Connectivity	• SC-7(10) Boundary Protection | Prevent Exfiltration • SC-10 Network Disconnect • SC-15(1) Collaborative Computing Devices | Physical or Logical Disconnect • SI-14(3) Non-Persistence | Non-Persistent Connectivity
	Unpredictability	Temporal Unpredictability	• SI-16 Memory Protection
Layer defenses and partition resources	Segmentation	Predefined Segmentation	• AC-4(2) Information Flow Enforcement | Processing Domains • AC-4(21) Information Flow Enforcement | Physical or Logical Separation of Information Flows • AC-6(4) Least Privilege| Separate Processing Domains • AU-9(2) Protection of Audit Information | Store on Separate Physical Systems and Components • CM-4(1) Impact Analyses | Separate Test Environments • CM-7(5) Least Functionality | Authorized Software

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
			• IA-2(13) Identification and Authentication | Out-Of-Band Authentication • MA-4(4) Nonlocal Maintenance | Authentication and Separation of Maintenance Sessions • SC-2 Separation of System and User Functionality • SC-2(1) Separation of System and User Functionality | Interfaces for Non-Privileged Users • SC-3 Security Function Isolation • SC-3(1) Security Function Isolation | Hardware Separation • SC-3(2) Security Function Isolation | Access and Flow Control Functions • SC-3(5) Security Function Isolation | Layered Structures • SC-7 Boundary Protection • SC-7(13) Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components • SC-7(15) Boundary Protection | Network Privileged Accesses • SC-7(21) Boundary Protection | Isolation of System Components • SC-7(22) Boundary Protection | Separate Subnets for Connecting to Different Security Domains • SC-11 Trusted Path • SC-32 System Partitioning • SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions • SC-39 Process Isolation • SC-39(1) Process Isolation | Hardware Separation • SC-39(2) Process Isolation | Separation Execution Domains Per Thread • SC-44 Detonation Chambers • SC-49 Hardware-Enforced Separation and Policy Enforcement • SC-50 Software-Enforced Separation and Policy Enforcement
		Dynamic Segmentation and Isolation	• CM-7(5) Least Functionality | Authorized Software • SC-7(20) Boundary Protection | Dynamic Isolation and Segregation • SC-18(5) Mobile Code | Allow Execution Only in Confined Environments • SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions • SC-39 Process Isolation • SC-39(1) Process Isolation | Hardware Separation • SC-39(2) Process Isolation | Separation Execution Domains Per Thread

3.6 CSA-06

CSA-06 – **Minimize and Harden Attack Surfaces**: System shall automatically disable all unauthorized ports, protocols, and services (PPS), including access points, by default. Any deviations from PPS baselines shall be approved and documented by a management board. System shall support automated monitoring and logging of system attack surface and associated cyber-events. Any removable media use must be approved, documented and strictly monitored. [1], [2], and [10]

Table 7. Cyber Resiliency Constructs Supporting CSA-06

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 controls
CR Strategic Design Principle: Reduce attack surfaces			
Limit the need for trust	Privilege Restriction	Trust-Based Privilege Management	• AC-3(2) Access Enforcement| Dual Authorization • AC-6(2) Least Privilege| Non-Privileged Access for Non-Security Functions • AC-6(3) Least Privilege| Network Access to Privileged Commands • AC-6(4) Least Privilege| Separate Processing Domains • AC-6(10) Least Privilege| Prohibit Non-Privileged Users from Executing Privileged Functions • CM-5(4) Access Restrictions for Change| Dual Authorization • CM-5(5) Access Restrictions for Change| Privilege Limitation for Production and Operation • CM-5(6) Access Restrictions for Change| Limit Library Privileges • CM-7(5) Least Functionality| Authorized Software – Allow-By-Exception • CP-9(7) System Backup| Dual Authorization
		Attribute-Based Usage Restriction	• AC-3(12) Access Enforcement | Assert and Enforce Application Access • AC-6 Least Privilege • AC-6(1) Least Privilege | Authorize Access to Security Functions • AC-6(4) Least Privilege | Separate Process Domains • AC-6(8) Least Privilege | Privilege Levels for Code Execution • AC-6(10) Least Privilege| Prohibit Non-Privileged Users from Executing Privileged Functions • RA-5(5) Vulnerability Monitoring and Scanning | Privileged Access
		Dynamic Privileges	• AC-6(8) Least Privilege | Privilege Levels for Code Execution • IA-10 Adaptive Authentication
	Realignment	Purposing	• AC-6(2) Least Privilege | Non-Privileged Access for Nonsecurity Functions • CM-7(4) Least Functionality | Unauthorized Software • CM-7(6) Least Functionality | Confined Environments with Limited Privileges • PM-32 Purposing
		Offloading	• PM-7(1) Enterprise Architecture | Offloading • SC-3(5) Security Function Isolation | Layered Structures • SC-7(15) Boundary Protection | Network Privileged Accesses • SC-25 Thin Nodes
		Restriction	• CM-2(7) Baseline Configuration | Configure Systems and Components for High-Risk Areas • CM-7(2) Least Functionality | Prevent Program Execution • SC-3(3) Security Function Isolation | Minimize Nonsecurity Functionality
		Replacement	• SA-11(6) Incident Handling | Supply Chain Coordination • SA-15(5) Development Process, Standards, And Tools | Attack Surface Reduction
		Specialization	• SA-20 Customized Development of Critical Components • SA-23 Specialization
Change or disrupt the attack surface	Non-Persistence	Non-Persistent Information	• SC-23(3) Session Authenticity | Unique System-Generated Session Identifiers • SC-25 Thin Nodes • SC-34(1) Non-Modifiable Executable Programs | No Writable Storage • SI-14(1) Non-Persistence | Refresh from Trusted Sources

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 controls
		Non-Persistent Services	• SC-25 Thin Nodes • SI-14 Non-Persistence • SI-14(1) Non-Persistence | Refresh from Trusted Sources
		Non-Persistent Connectivity	• SC-10 Network Disconnect • SC-15(1) Collaborative Computing Devices | Physical or Logical Disconnect • SI-14(3) Non-Persistence | Non-Persistent Connectivity
Make the effects of deception and unpredictability user-transparent	Coordinated Protection	Calibrated Defense-in-Depth	• IA-10 Adaptive Authentication • PL-8(1) Security and Privacy Architecture | Defense in Depth
		Orchestration	• SC-3(5) Security Function Isolation | Layered Structures
		Self-Challenge	• CA-8 Penetration Testing • CA-8(1) Penetration Testing | Independent Penetration Testing Agent or Team • CA-8(2) Penetration Testing | Red Team Exercises • CA-8(3) Penetration Testing | Facility Penetration Testing • CP-4(5) Self-Challenge • SA-11(5) Developer Testing and Evaluation | Penetration Testing • SR-6(1) Supplier Assessments and Reviews | Penetration Testing and Analysis
Determine on-going trustworthiness	Substantiated Integrity	Integrity Checks	• CM-14 Signed Components • IA-3(1) Device Identification and Authentication | Cryptographic Bidirectional Authentication • PE-3(5) Physical Access Control | Tamper Protection • SC-8(1) Transmission Confidentiality and Integrity | Cryptographic Protection • SC-8(5) Transmission Confidentiality and Integrity | Protected Distribution System • SC-28(1) Protection of Information at Rest | Cryptographic Protection • SC-34 Non-Modifiable Executable Programs • SC-34(2) Non-Modifiable Executable Programs | Integrity Protection on Read-Only Media • SC-51 Hardware-Based Protection • SI-6 Security and Privacy Function Verification • SI-7 Software, Firmware, and Information Integrity • SI-7(1) Software, Firmware, and Information Integrity | Integrity Checks • SI-7(6) Software, Firmware, and Information Integrity | Cryptographic Protection • SI-7(9) Software, Firmware, and Information Integrity | Verify Boot Process • SI-7(10) Software, Firmware, and Information Integrity | Protection of Boot Firmware • SI-7(12) Software, Firmware, and Information Integrity | Integrity Verification • SR-4(3) Provenance | Validate as Genuine and Not Altered • SR-9 Tamper Resistance and Detection • SR-9(1) Tamper Resistance and Detection | Multiple Stages of System Development Life Cycle
		Provenance Tracking	• CM-14 Signed Components • SC-7(11) Boundary Protection | Restrict Incoming Communications Traffic • SC-11 Trusted Path • SI-7(15) Software, Firmware, And Information Integrity | Code Authentication

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 controls
			• SI-10(5) Information Input Validation | Restrict Inputs to Trusted Sources and Approved Formats • SI-14(1) Non-Persistence | Refresh from Trusted Sources • SR-4 Provenance • SR-4(3) Provenance | Validate as Genuine and Not Altered • SR-11 Component Authenticity
		Behavior Validation	• SI-10(3) Information Input Validation |Predictable Behavior • SR-10 Inspection of Systems or Components • SR-11 Component Authenticity
Contain and exclude behaviors	Privilege Restriction	Trust-Based Privilege Management	• AC-3(2) Access Enforcement| Dual Authorization • AC-6(2) Least Privilege| Non-Privileged Access for Non-Security Functions • AC-6(3) Least Privilege| Network Access to Privileged Commands • AC-6(4) Least Privilege| Separate Processing Domains • AC-6(10) Least Privilege| Prohibit Non-Privileged Users from Executing Privileged Functions • CM-5(4) Access Restrictions for Change| Dual Authorization • CM-5(5) Access Restrictions for Change| Privilege Limitation for Production and Operation • CM-5(6) Access Restrictions for Change| Limit Library Privileges • CM-7(5) Least Functionality| Authorized Software – Allow-By-Exception • CP-9(7) System Backup| Dual Authorization
		Attribute-Based Usage Restriction	• AC-3(12) Access Enforcement | Assert and Enforce Application Access • AC-6 Least Privilege • AC-6(1) Least Privilege | Authorize Access to Security Functions • AC-6(4) Least Privilege | Separate Process Domains • AC-6(8) Least Privilege | Privilege Levels for Code Execution • AC-6(10) Least Privilege| Prohibit Non-Privileged Users from Executing Privileged Functions • RA-5(5) Vulnerability Monitoring and Scanning | Privileged Access
		Dynamic Privileges	• AC-6(8) Least Privilege | Privilege Levels for Code Execution • IA-10 Adaptive Authentication
	Segmentation	Predefined Segmentation	• AC-4(21) Information Flow Enforcement | Physical or Logical Separation of Information Flows • AC-6(4) Least Privilege| Separate Processing Domains • CM-4(1) Impact Analyses | Separate Test Environments • CM-7(5) Least Functionality | Authorized Software • SC-2 Separation of System and User Functionality • SC-2(1) Separation of System and User Functionality | Interfaces for Non-Privileged Users • SC-3 Security Function Isolation • SC-3(1) Security Function Isolation | Hardware Separation • SC-3(2) Security Function Isolation | Access and Flow Control Functions • SC-3(5) Security Function Isolation | Layered Structures • SC-7 Boundary Protection • SC-7(13) Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components • SC-7(15) Boundary Protection | Network Privileged Accesses • SC-7(21) Boundary Protection | Isolation of System Components • SC-7(22) Boundary Protection | Separate Subnets for Connecting to Different Security Domains • SC-8(5) Transmission Confidentiality and Integrity | Protected Distribution System • SC-11 Trusted Path

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 controls
			• SC-32 System Partitioning • SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions • SC-39 Process Isolation • SC-39(1) Process Isolation | Hardware Separation • SC-39(2) Process Isolation | Separation Execution Domains Per Thread • SC-44 Detonation Chambers • SC-49 Hardware-Enforced Separation and Policy Enforcement • SC-50 Software-Enforced Separation and Policy Enforcement
		Dynamic Segmentation and Isolation	• CM-7(5) Least Functionality | Authorized Software • SC-7(20) Boundary Protection | Dynamic Isolation and Segregation • SC-18(5) Mobile Code | Allow Execution Only in Confined Environments • SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions • SC-35 External Malicious Code Identification • SC-39 Process Isolation • SC-39(1) Process Isolation | Hardware Separation • SC-39(2) Process Isolation | Separation Execution Domains Per Thread
Layer defenses and partition resources	Coordinated Protection	Calibrated Defense-in-Depth	• IA-10 Adaptive Authentication • PL-8(1) Security and Privacy Architecture | Defense in Depth
		Orchestration	• SC-3(5) Security Function Isolation | Layered Structures
		Self-Challenge	• CA-8 Penetration Testing • CA-8(1) Penetration Testing | Independent Penetration Testing Agent or Team • CA-8(2) Penetration Testing | Red Team Exercises • CA-8(3) Penetration Testing | Facility Penetration Testing • CP-4(5) Self-Challenge • SA-11(5) Developer Testing and Evaluation | Penetration Testing • SR-6(1) Supplier Assessments and Reviews | Penetration Testing and Analysis
	Segmentation	Predefined Segmentation	• AC-4(21) Information Flow Enforcement | Physical or Logical Separation of Information Flows • AC-6(4) Least Privilege| Separate Processing Domains • CM-4(1) Impact Analyses | Separate Test Environments • CM-7(5) Least Functionality | Authorized Software • SC-2 Separation of System and User Functionality • SC-2(1) Separation of System and User Functionality | Interfaces for Non-Privileged Users • SC-3 Security Function Isolation • SC-3(1) Security Function Isolation | Hardware Separation • SC-3(2) Security Function Isolation | Access and Flow Control Functions • SC-3(5) Security Function Isolation | Layered Structures • SC-7 Boundary Protection • SC-7(13) Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components • SC-7(15) Boundary Protection | Network Privileged Accesses • SC-7(21) Boundary Protection | Isolation of System Components • SC-7(22) Boundary Protection | Separate Subnets for Connecting to Different Security Domains • SC-8(5) Transmission Confidentiality and Integrity | Protected Distribution System • SC-11 Trusted Path • SC-32 System Partitioning

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 controls
			• SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions • SC-39 Process Isolation • SC-39(1) Process Isolation | Hardware Separation • SC-39(2) Process Isolation | Separation Execution Domains Per Thread • SC-44 Detonation Chambers • SC-49 Hardware-Enforced Separation and Policy Enforcement • SC-50 Software-Enforced Separation and Policy Enforcement
		Dynamic Segmentation and Isolation	• CM-7(5) Least Functionality | Authorized Software • SC-7(20) Boundary Protection | Dynamic Isolation and Segregation • SC-18(5) Mobile Code | Allow Execution Only in Confined Environments • SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions • SC-35 External Malicious Code Identification • SC-39 Process Isolation • SC-39(1) Process Isolation | Hardware Separation • SC-39(2) Process Isolation | Separation Execution Domains Per Thread
CR Strategic Design Principle: Expect adversaries to evolve			
Contain and exclude behaviors	Privilege Restriction	Trust-Based Privilege Management	• AC-3(2) Access Enforcement| Dual Authorization • AC-6(2) Least Privilege| Non-Privileged Access for Non-Security Functions • AC-6(3) Least Privilege| Network Access to Privileged Commands • AC-6(4) Least Privilege| Separate Processing Domains • AC-6(10) Least Privilege| Prohibit Non-Privileged Users from Executing Privileged Functions • CM-5(4) Access Restrictions for Change| Dual Authorization • CM-5(5) Access Restrictions for Change| Privilege Limitation for Production and Operation • CM-5(6) Access Restrictions for Change| Limit Library Privileges • CM-7(5) Least Functionality| Authorized Software – Allow-By-Exception • CP-9(7) System Backup| Dual Authorization
		Attribute-Based Usage Restriction	• AC-3(12) Access Enforcement | Assert and Enforce Application Access • AC-6 Least Privilege • AC-6(1) Least Privilege | Authorize Access to Security Functions • AC-6(4) Least Privilege | Separate Process Domains • AC-6(8) Least Privilege | Privilege Levels for Code Execution • AC-6(10) Least Privilege| Prohibit Non-Privileged Users from Executing Privileged Functions • RA-5(5) Vulnerability Monitoring and Scanning | Privileged Access
		Dynamic Privileges	• AC-6(8) Least Privilege | Privilege Levels for Code Execution • IA-10 Adaptive Authentication
	Segmentation	Predefined Segmentation	• AC-4(21) Information Flow Enforcement | Physical or Logical Separation of Information Flows • AC-6(4) Least Privilege| Separate Processing Domains • CM-4(1) Impact Analyses | Separate Test Environments • CM-7(5) Least Functionality | Authorized Software • SC-2 Separation of System and User Functionality • SC-2(1) Separation of System and User Functionality | Interfaces for Non-Privileged Users • SC-3 Security Function Isolation • SC-3(1) Security Function Isolation | Hardware Separation • SC-3(2) Security Function Isolation | Access and Flow Control Functions • SC-3(5) Security Function Isolation | Layered Structures • SC-7 Boundary Protection

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 controls
			• SC-7(13) Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components • SC-7(15) Boundary Protection | Network Privileged Accesses • SC-7(21) Boundary Protection | Isolation of System Components • SC-7(22) Boundary Protection | Separate Subnets for Connecting to Different Security Domains • SC-8(5) Transmission Confidentiality and Integrity | Protected Distribution System • SC-11 Trusted Path • SC-32 System Partitioning • SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions • SC-39 Process Isolation • SC-39(1) Process Isolation | Hardware Separation • SC-39(2) Process Isolation | Separation Execution Domains Per Thread • SC-44 Detonation Chambers • SC-49 Hardware-Enforced Separation and Policy Enforcement • SC-50 Software-Enforced Separation and Policy Enforcement
		Dynamic Segmentation and Isolation	• CM-7(5) Least Functionality | Authorized Software • SC-7(20) Boundary Protection | Dynamic Isolation and Segregation • SC-18(5) Mobile Code | Allow Execution Only in Confined Environments • SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions • SC-35 External Malicious Code Identification • SC-39 Process Isolation • SC-39(1) Process Isolation | Hardware Separation • SC-39(2) Process Isolation | Separation Execution Domains Per Thread
CR Strategic Design Principle: Assume compromised resources			
Leverage health and status data	Analytic Monitoring	Monitoring and Damage Assessment	• CM-2(7) Baseline Configuration | Configure Systems and Components for High-Risk Areas • CM-8(3) System Component Inventory | Automated Unauthorized Component Detection • RA-5(5) Vulnerability Monitoring and Scanning | Privileged Access • SC-26 Decoys • SI-4(7) System Monitoring | Automated Response to Suspicious Events • SR-6(1) Supplier Assessments and Reviews | Penetration Testing and Analysis
		Forensic and Behavioral Analysis	• CM-2(7) Baseline Configuration | Configure Systems and Components for High-Risk Areas • SC-26 Decoys • SC-44 Detonation Chambers • SR-10 Inspection of Systems or Components

3.7 CSA-07

CSA-07 – **Baseline & Monitor Systems and Detect Anomalies**: System shall implement and maintain a cyber survivability configuration baseline for its GOTS/COTS HW, SW, FW and open source modules, by version number to ensure an operationally acceptable cyber risk posture 24/7 (note: drives CDRLs). System shall monitor, detect and report system health status and anomalies indicative of cyber events, based on its current adversary cyber threat intelligence, CONOPS, and Mission Relevant Cyber Terrain (MRT-C). Applicable report detail shall be provided to users, system operators and assigned cyber defenders (e.g., system shall report

anomalies such as configuration changes, cyber-related event indicators, slowed processing, or loss of functionality within T = (# of seconds/minutes [specified by sponsor]). [1], [2], and [10]

The amount of data available for monitoring may be overwhelming, complicating the task of identifying critical information. One way of reducing the amount of data without impacting mission is to focus the mission requirements on common critical assets and the impacts of these assets on missions.

Table 8. Cyber Resiliency Constructs Supporting CSA-07

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 controls
CR Strategic Design Principle: Focus on common critical assets			
Leverage health and status data	Analytic Monitoring	Monitoring and Damage Assessment	• AC-2(12) Account Management | Account Monitoring for Atypical Usage • AC-23 Data Mining Protection • AU-6 Audit Record Review, Analysis, and Reporting • AU-6(8) Audit Record Review, Analysis, And Reporting | Full Text Analysis of Privileged Commands • CM-8(3) System Component Inventory | Automated Unauthorized Component Detection • IR-4(13) Incident Handling | Behavior Analysis • IR-5 Incident Monitoring • PE-6 Monitoring Physical Access • PE-6(2) Monitoring Physical Access | Automated Intrusion Recognition and Responses • PE-6(4) Monitoring Physical Access | Monitoring Physical Access to Systems • PM-31 Continuous Monitoring Strategy • RA-5(5) Vulnerability Monitoring and Scanning | Privileged Access • RA-10 Threat Hunting • SC-5(3) Denial of Service Protection | Detection and Monitoring • SC-26 Decoys • SC-35 External Malicious Code Identification • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis • SI-4(3) System Monitoring | Automated Tool and Mechanism Integration • SI-4(4) System Monitoring | Inbound and Outbound Communications Traffic • SI-4(7) System Monitoring | Automated Response to Suspicious Events • SI-4(10) System Monitoring | Visibility of Encrypted Communications • SI-4(11) System Monitoring | Analyze Communications Traffic Anomalies • SI-4(13) System Monitoring | Analyze Traffic and Event Patterns • SI-4(18) System Monitoring | Analyze Traffic and Covert Exfiltration • SI-7(7) Software, Firmware, and Information Integrity | Integration of Detection and Response • SR-6(1) Supplier Assessments and Reviews | Penetration Testing and Analysis • SR-10 Inspection of Systems or Components
		Sensor Fusion and Analysis	• AU-6(3) Audit Record Review, Analysis, and Reporting | Correlate Audit Repositories • AU-6(5) Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records • AU-6(6) Audit Record Review, Analysis, and Reporting | Correlation with Physical Monitoring

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 controls
			• AU-6(9) Audit Record Review, Analysis, And Reporting | Correlation with Information from Nontechnical Sources • IR-4(4) Incident Handling | Information Correlation • PM-31 Continuous Monitoring Strategy • RA-5(6) Vulnerability Monitoring and Scanning | Automated Trend Analyses • RA-5(8) Vulnerability Monitoring and Scanning | Review Historic Audit Logs • RA-5(10) Vulnerability Monitoring and Scanning | Correlate Scanning Information • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis • SI-4(3) System Monitoring | Automated Tool and Mechanism Integration • SI-4(16) System Monitoring | Correlate Monitoring Information • SI-4(17) System Monitoring | Integrated Situational Awareness • SI-4(24) System Monitoring | Indicators of Compromise • SI-4(25) System Monitoring | Optimize Network Traffic Analysis
		Forensic and Behavioral Analysis	• CM-2(7) Baseline Configuration | Configure Systems and Components for High-Risk Areas • IR-4(11) Incident Handling | Integrated Incident Response Team • IR-4(12) Incident Handling | Malicious Code and Forensic Analysis • IR-5 Incident Monitoring • SC-26 Decoys • SC-35 External Malicious Code Identification • SC-44 Detonation Chambers • SI-3(10) Malicious Code Protection | Malicious Code Analysis • SR-10 Inspection of Systems or Components
	Contextual Awareness	Dynamic Resource Awareness	• CA-7(3) Continuous Monitoring | Trend Analyses • SI-4(16) System Monitoring | Correlate Monitoring Information • SI-4(17) System Monitoring | Integrated Situational Awareness
		Dynamic Threat Awareness	• CA-7(3) Continuous Monitoring | Trend Analyses • IR-4(4) Incident Handling | Information Correlation • PM-16 Threat Awareness Program • PM-16(1) Threat Awareness Program | Automated Means for Sharing Threat Intelligence • RA-3(3) Risk Assessment | Dynamic Threat Awareness • RA-10 Threat Hunting • SA-11(2) Developer Testing and Evaluation | Threat Modeling and Vulnerability Analysis
		Mission Dependency and Status Visualization	• CP-2(8) Contingency Plan | Identify Critical Assets • RA-9 Criticality Analysis • SI-4(1) System Monitoring | System-Wide Intrusion Detection System • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis
Maintain situational awareness	Analytic Monitoring	Monitoring and Damage Assessment	• AC-2(12) Account Management | Account Monitoring for Atypical Usage • AC-23 Data Mining Protection • AU-6 Audit Record Review, Analysis, and Reporting • AU-6(8) Audit Record Review, Analysis, And Reporting | Full Text Analysis of Privileged Commands • CM-8(3) System Component Inventory | Automated Unauthorized Component Detection • IR-4(13) Incident Handling | Behavior Analysis • IR-5 Incident Monitoring

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 controls
			• PE-6 Monitoring Physical Access • PE-6(2) Monitoring Physical Access | Automated Intrusion Recognition and Responses • PE-6(4) Monitoring Physical Access | Monitoring Physical Access to Systems • PM-31 Continuous Monitoring Strategy • RA-5(5) Vulnerability Monitoring and Scanning | Privileged Access • RA-10 Threat Hunting • SC-5(3) Denial of Service Protection | Detection and Monitoring • SC-26 Decoys • SC-35 External Malicious Code Identification • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis • SI-4(3) System Monitoring | Automated Tool and Mechanism Integration • SI-4(4) System Monitoring | Inbound and Outbound Communications Traffic • SI-4(7) System Monitoring | Automated Response to Suspicious Events • SI-4(10) System Monitoring | Visibility of Encrypted Communications • SI-4(11) System Monitoring | Analyze Communications Traffic Anomalies • SI-4(13) System Monitoring | Analyze Traffic and Event Patterns • SI-4(18) System Monitoring | Analyze Traffic and Covert Exfiltration • SI-7(7) Software, Firmware, and Information Integrity | Integration of Detection and Response • SR-6(1) Supplier Assessments and Reviews | Penetration Testing and Analysis • SR-10 Inspection of Systems or Components
		Sensor Fusion and Analysis	• AU-6(3) Audit Record Review, Analysis, and Reporting | Correlate Audit Repositories • AU-6(5) Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records • AU-6(6) Audit Record Review, Analysis, and Reporting | Correlation with Physical Monitoring • AU-6(9) Audit Record Review, Analysis, And Reporting | Correlation with Information from Nontechnical Sources • IR-4(4) Incident Handling | Information Correlation • PM-31 Continuous Monitoring Strategy • RA-5(6) Vulnerability Monitoring and Scanning | Automated Trend Analyses • RA-5(8) Vulnerability Monitoring and Scanning | Review Historic Audit Logs • RA-5(10) Vulnerability Monitoring and Scanning | Correlate Scanning Information • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis • SI-4(3) System Monitoring | Automated Tool and Mechanism Integration • SI-4(16) System Monitoring | Correlate Monitoring Information • SI-4(17) System Monitoring | Integrated Situational Awareness • SI-4(24) System Monitoring | Indicators of Compromise • SI-4(25) System Monitoring | Optimize Network Traffic Analysis
		Forensic and Behavioral Analysis	• IR-4(11) Incident Handling | Integrated Incident Response Team • IR-4(12) Incident Handling | Malicious Code and Forensic Analysis • IR-5 Incident Monitoring • SC-26 Decoys

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 controls
			• SC-35 External Malicious Code Identification • SC-44 Detonation Chambers • SI-3(10) Malicious Code Protection | Malicious Code Analysis • SR-10 Inspection of Systems or Components
	Contextual Awareness	Dynamic Resource Awareness	• CA-7(3) Continuous Monitoring | Trend Analyses • SI-4(16) System Monitoring | Correlate Monitoring Information • SI-4(17) System Monitoring | Integrated Situational Awareness
		Dynamic Threat Awareness	• CA-7(3) Continuous Monitoring | Trend Analyses • IR-4(4) Incident Handling | Information Correlation • PM-16 Threat Awareness Program • PM-16(1) Threat Awareness Program | Automated Means for Sharing Threat Intelligence • RA-3(3) Risk Assessment | Dynamic Threat Awareness • RA-10 Threat Hunting • SA-11(2) Developer Testing and Evaluation | Threat Modeling and Vulnerability Analysis
		Mission Dependency and Status Visualization	• CP-2(8) Contingency Plan | Identify Critical Assets • RA-9 Criticality Analysis • SI-4(1) System Monitoring | System-Wide Intrusion Detection System • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis

3.8 CSA-08

CSA-08 – **Manage System Performance and Enable Cyberspace Defense**: If anomalies are detected and/or cyber-events degrade system capability, the system shall be sufficiently resilient to mitigate cyber-related event effects through orderly, structured and prioritized system responses, in order to ensure minimum mission functionality requirements [system functionality threshold specified by sponsor] to complete the current mission or return for recovery. The system shall enable assigned cyber defenders to impose effects on adversaries to counter their operations and objectives. Alternatively, the mission commander shall be able to selectively disconnect/disable subsystems that are not critical as well as isolate the system from integrated platform systems and/or the Department of Defense Information Network (DoDIN). [1], [2], and [10]

Table 9. Cyber Resiliency Constructs Supporting CSA-08

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
CR Strategic Design Principle: Focus on common critical assets			
Control visibility and use	Privilege Restriction	Trust-Based Privilege Management	• AU-9(6) Protection of Audit Information| Read-Only Access
		Attribute-Based Usage Restriction	• AC-3(11) Access Enforcement | Restrict Access to Specific Information Types • AC-3(12) Access Enforcement | Assert and Enforce Application Access • AC-3(13) Access Enforcement | Dynamic Information Flow control • AC-6 Least Privilege • AC-6(1) Least Privilege | Authorize Access to Security Functions • AU-9(6) Protection of Audit Information| Read-Only Access

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
		Dynamic Privileges	• AC-2(6) Account Management | Dynamic Privilege Management • AC-2(8) Account Management | Dynamic Account Management • IA-10 Adaptive Authentication
	Segmentation	Predefined Segmentation	• AU-9(2) Protection of Audit Information | Store on Separate Physical Systems and Components • IA-2(13) Identification and Authentication | Out-Of-Band Authentication • IR-4(12) Incident Handling | Malicious Code and Forensic Analysis • SC-7 Boundary Protection • SC-7(13) Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components • SC-7(21) Boundary Protection | Isolation of System Components • SC-7(22) Boundary Protection | Separate Subnets for Connecting to Different Security Domains • SC-32 System Partitioning • SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions • SC-39 Process Isolation • SC-39(1) Process Isolation | Hardware Separation • SC-39(2) Process Isolation | Separation Execution Domains Per Thread • SC-49 Hardware-Enforced Separation and Policy Enforcement • SC-50 Software-Enforced Separation and Policy Enforcement
		Dynamic Segmentation and Isolation	• SC-7(20) Boundary Protection | Dynamic Isolation and Segregation • SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions • SC-39 Process Isolation • SC-39(1) Process Isolation | Hardware Separation • SC-39(2) Process Isolation | Separation Execution Domains Per Thread
Contain and exclude behaviors	Privilege Restriction	Trust-Based Privilege Management	• AU-9(6) Protection of Audit Information| Read-Only Access
		Attribute-Based Usage Restriction	• AC-3(11) Access Enforcement | Restrict Access to Specific Information Types • AC-3(12) Access Enforcement | Assert and Enforce Application Access • AC-3(13) Access Enforcement | Dynamic Information Flow control • AC-6 Least Privilege • AC-6(1) Least Privilege | Authorize Access to Security Functions • AU-9(6) Protection of Audit Information| Read-Only Access
		Dynamic Privileges	• AC-2(6) Account Management | Dynamic Privilege Management • AC-2(8) Account Management | Dynamic Account Management • IA-10 Adaptive Authentication
	Segmentation	Predefined Segmentation	• AU-9(2) Protection of Audit Information | Store on Separate Physical Systems and Components • IA-2(13) Identification and Authentication | Out-Of-Band Authentication • IR-4(12) Incident Handling | Malicious Code and Forensic Analysis • SC-7 Boundary Protection • SC-7(13) Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components • SC-7(21) Boundary Protection | Isolation of System Components • SC-7(22) Boundary Protection | Separate Subnets for Connecting to Different Security Domains • SC-32 System Partitioning • SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
			• SC-39 Process Isolation • SC-39(1) Process Isolation | Hardware Separation • SC-39(2) Process Isolation | Separation Execution Domains Per Thread • SC-49 Hardware-Enforced Separation and Policy Enforcement • SC-50 Software-Enforced Separation and Policy Enforcement
		Dynamic Segmentation and Isolation	• SC-7(20) Boundary Protection | Dynamic Isolation and Segregation • SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions • SC-39 Process Isolation • SC-39(1) Process Isolation | Hardware Separation • SC-39(2) Process Isolation | Separation Execution Domains Per Thread
Maintain situational awareness	Contextual Awareness	Dynamic Resource Awareness	• SI-4(16) System Monitoring | Correlate Monitoring Information • SI-4(17) System Monitoring | Integrated Situational Awareness
		Dynamic Threat Awareness	• IR-4(4) Incident Handling | Information Correlation • RA-3(3) Risk Assessment | Dynamic Threat Awareness • RA-10 Threat Hunting
		Mission Dependency and Status Visualization	• CP-2(8) Contingency Plan | Identify Critical Assets • RA-9 Criticality Analysis • SI-4(1) System Monitoring | System-Wide Intrusion Detection System • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis
Maintain redundancy	Redundancy	Protected Backup and Restore	• CP-9 System Backup • CP-9(8) System Backup | Cryptographic Protection
		Surplus Capacity	• SC-5(2) Denial of Service Protection | Capacity, Bandwidth, and Redundancy
		Replication	• CP-9(6) System Backup | Redundant Secondary System • PE-9(1) Power Equipment and Cabling | Redundant Cabling • PE-11(1) Emergency Power | Alternate Power Supply – Minimal Operational Capability • PE-11(2) Emergency Power | Alternate Power Supply – Self-Contained • PE-17 Alternate Work Site • SC-36 Distributed Processing and Storage • SC-36(2) Distributed Processing and Storage | Synchronization • SR-5(1) Acquisition Strategies, Tools, and Methods | Adequate Supply
CR Strategic Design Principle: Support agility and architect for adaptability			
Plan and manage diversity	Diversity	Architectural Diversity	• AU-9(7) Protection of Audit Information | Store on Component with Different Operating System • CP-8(3) Telecommunications Services | Separation of Primary and Alternate Providers • CP-11 Alternate Communications Protocols • CP-13 Alternative Security Mechanisms • SC-29 Heterogeneity • SC-29(1) Heterogeneity | Virtualization Techniques
		Design Diversity	• CP-11 Alternate Communications Protocols • CP-13 Alternative Security Mechanisms • SA-17(9) Developer Security Architecture and Design | Design Diversity
		Synthetic Diversity	• SI-16 Memory Protection
		Information Diversity	• SI-22 Information Diversity
		Path Diversity	• AC-7(4) Unsuccessful Logon Attempts | Use of Alternate Authentication Factor

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
			• IA-2(13) Identification and Authentication | Out-Of-Band Authentication • SC-37 Out-Of-Band Channels • SC-47 Alternate Communication Paths
		Supply Chain Diversity	• PL-8(2) Security and Privacy Architecture | Supplier Diversity • SR-3(1) Supply Chain Controls and Processes | Diverse Supply Chain • SR-5(1) Acquisition Strategies, Tools, and Methods | Adequate Supply
Maintain redundancy	Redundancy	Protected Backup and Restore	• CP-9 System Backup • CP-9(8) System Backup | Cryptographic Protection
		Surplus Capacity	• SC-5(2) Denial of Service Protection | Capacity, Bandwidth, and Redundancy
		Replication	• CP-9(6) System Backup | Redundant Secondary System • PE-9(1) Power Equipment and Cabling | Redundant Cabling • PE-11(1) Emergency Power | Alternate Power Supply – Minimal Operational Capability • PE-11(2) Emergency Power | Alternate Power Supply – Self-Contained • PE-17 Alternate Work Site • SC-36 Distributed Processing and Storage • SC-36(2) Distributed Processing and Storage | Synchronization • SR-5(1) Acquisition Strategies, Tools, and Methods | Adequate Supply
Leverage health and status data	Analytic Monitoring	Monitoring and Damage Assessment	• AC-2(12) Account Management | Account Monitoring for Atypical Usage • CM-8(3) System Component Inventory | Automated Unauthorized Component Detection • IR-4(13) Incident Handling | Behavior Analysis • IR-5 Incident Monitoring • PE-6 Monitoring Physical Access • PE-6(2) Monitoring Physical Access | Automated Intrusion Recognition and Responses • PE-6(4) Monitoring Physical Access | Monitoring Physical Access to Systems • PM-31 Continuous Monitoring Strategy • RA-10 Threat Hunting • SC-5(3) Denial of Service Protection | Detection and Monitoring • SC-26 Decoys • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis • SI-4(3) System Monitoring | Automated Tool and Mechanism Integration • SI-4(4) System Monitoring | Inbound and Outbound Communications Traffic • SI-4(7) System Monitoring | Automated Response to Suspicious Events • SI-4(11) System Monitoring | Analyze Communications Traffic Anomalies • SI-4(13) System Monitoring | Analyze Traffic and Event Patterns • SI-4(18) System Monitoring | Analyze Traffic and Covert Exfiltration • SI-7(7) Software, Firmware, and Information Integrity | Integration of Detection and Response
		Sensor Fusion and Analysis	• IR-4(4) Incident Handling | Information Correlation • PM-31 Continuous Monitoring Strategy • RA-5(10) Vulnerability Monitoring and Scanning | Correlate Scanning Information • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
			• SI-4(3) System Monitoring | Automated Tool and Mechanism Integration • SI-4(16) System Monitoring | Correlate Monitoring Information • SI-4(17) System Monitoring | Integrated Situational Awareness • SI-4(24) System Monitoring | Indicators of Compromise
		Forensic and Behavioral Analysis	• IR-4(11) Incident Handling | Integrated Incident Response Team • IR-4(12) Incident Handling | Malicious Code and Forensic Analysis • IR-5 Incident Monitoring • SC-26 Decoys • SI-3(10) Malicious Code Protection | Malicious Code Analysis
Manage resources (risk-) adaptively	Contextual Awareness	Dynamic Resource Awareness	• SI-4(16) System Monitoring | Correlate Monitoring Information • SI-4(17) System Monitoring | Integrated Situational Awareness
		Dynamic Threat Awareness	• IR-4(4) Incident Handling | Information Correlation • RA-3(3) Risk Assessment | Dynamic Threat Awareness • RA-10 Threat Hunting
		Mission Dependency and Status Visualization	• CP-2(8) Contingency Plan | Identify Critical Assets • RA-9 Criticality Analysis • SI-4(1) System Monitoring | System-Wide Intrusion Detection System • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis
CR Strategic Design Principle: Expect adversaries to evolve			
Manage resources (risk-) adaptively	Adaptive Response	Dynamic Reconfiguration	• AC-2(6) Account Management | Dynamic Privilege Management • AC-2(8) Account Management | Dynamic Account Management • AC-4(3) Information Flow Enforcement | Dynamic Information Flow Control • CP-2(5) Contingency Plan | Continue Missions and Business Functions • IR-4(2) Incident Handling | Dynamic Reconfiguration • IR-4(3) Incident Handling | Continuity of Operations • IR-4(9) Incident Handling | Dynamic Response Capability • IR-4(11) Incident Handling | Integrated Incident Response Team • SC-7(20) Boundary Protection | Dynamic Isolation and Segregation
		Dynamic Resource Allocation	• AC-2(8) Account Management | Dynamic Account Management • AU-5(3) Response to Audit Processing Failures | Configurable Traffic Volume Thresholds • SC-5(2) Denial of Service Protection | Capacity, Bandwidth, and Redundancy
		Adaptive Management	• AC-2(8) Account Management | Dynamic Account Management • AC-4(3) Information Flow Enforcement | Dynamic Information Flow Control • AU-5(3) Response to Audit Processing Failures | Configurable Traffic Volume Thresholds • CP-2(5) Contingency Plan | Continue Missions and Business Functions • CP-12 Safe Mode • CP-13 Alternative Security Mechanisms • IA-10 Adaptive Authentication • IR-4(3) Incident Handling | Continuity of Operations • IR-4(11) Incident Handling | Integrated Incident Response Team • PE-6(2) Monitoring Physical Access | Automated Intrusion Recognition and Responses • RA-3(3) Risk Assessment | Dynamic Threat Awareness • SI-4(3) System Monitoring | Automated Tool and Mechanism Integration • SI-4(7) System Monitoring | Automated Response to Suspicious Events

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
			• SI-7(5) Software, Firmware, and Information Integrity | Automated Response to Integrity Violations
	Coordinated Protection	Calibrated Defense-in-Depth	• IA-2(13) Identification and Authentication | Out-Of-Band Authentication • IA-10 Adaptive Authentication • PE-6(4) Monitoring Physical Access | Monitoring Physical Access to Systems • PL-8(1) Security and Privacy Architecture | Defense in Depth
		Consistency Analysis	• CA-7(5) Continuous Monitoring | Consistency Analysis
		Orchestration	• CP-2(5) Contingency Plan | Continue Missions and Business Functions • IA-2(13) Identification and Authentication | Out-Of-Band Authentication • IR-4(3) Incident Handling | Continuity of Operations • IR-4(4) Incident Handling | Information Correlation • IR-4(11) Incident Handling | Integrated Incident Response Team • PE-6(2) Monitoring Physical Access | Automated Intrusion Recognition and Responses
		Self-Challenge	• CP-4(5) Self-Challenge
Determine ongoing trustworthiness	Adaptive Response	Dynamic Reconfiguration	• AC-2(6) Account Management | Dynamic Privilege Management • AC-2(8) Account Management | Dynamic Account Management • AC-4(3) Information Flow Enforcement | Dynamic Information Flow Control • CP-2(5) Contingency Plan | Continue Missions and Business Functions • IR-4(2) Incident Handling | Dynamic Reconfiguration • IR-4(3) Incident Handling | Continuity of Operations • IR-4(9) Incident Handling | Dynamic Response Capability • IR-4(11) Incident Handling | Integrated Incident Response Team • SC-7(20) Boundary Protection | Dynamic Isolation and Segregation
		Dynamic Resource Allocation	• AC-2(8) Account Management | Dynamic Account Management • AU-5(3) Response to Audit Processing Failures | Configurable Traffic Volume Thresholds • SC-5(2) Denial of Service Protection | Capacity, Bandwidth, and Redundancy
		Adaptive Management	• AC-2(8) Account Management | Dynamic Account Management • AC-4(3) Information Flow Enforcement | Dynamic Information Flow Control • AU-5(3) Response to Audit Processing Failures | Configurable Traffic Volume Thresholds • CP-2(5) Contingency Plan | Continue Missions and Business Functions • CP-12 Safe Mode • CP-13 Alternative Security Mechanisms • IA-10 Adaptive Authentication • IR-4(3) Incident Handling | Continuity of Operations • IR-4(11) Incident Handling | Integrated Incident Response Team • PE-6(2) Monitoring Physical Access | Automated Intrusion Recognition and Responses • RA-3(3) Risk Assessment | Dynamic Threat Awareness • SI-4(3) System Monitoring | Automated Tool and Mechanism Integration • SI-4(7) System Monitoring | Automated Response to Suspicious Events • SI-7(5) Software, Firmware, and Information Integrity | Automated Response to Integrity Violations
	Substantiated Integrity	Integrity Checks	• AU-9(1) Protection of Audit Information | Hardware Write-Once Media • AU-9(3) Protection of Audit Information | Cryptographic Protection • AU-9(6) Protection of Audit Information | Read-Only Access

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
			• SC-28(1) Protection of Information at Rest | Cryptographic Protection • SC-34 Non-Modifiable Executable Programs • SC-34(2) Non-Modifiable Executable Programs | Integrity Protection on Read-Only Media • SC-51 Hardware-Based Protection • SI-6 Security and Privacy Function Verification • SI-7 Software, Firmware, and Information Integrity • SI-7(1) Software, Firmware, and Information Integrity | Integrity Checks • SI-7(5) Software, Firmware, and Information Integrity | Automated Response to Integrity Violations • SI-7(6) Software, Firmware, and Information Integrity | Cryptographic Protection • SI-7(7) Software, Firmware, and Information Integrity | Integration of Detection and Response • SI-7(9) Software, Firmware, and Information Integrity | Verify Boot Process • SI-7(10) Software, Firmware, and Information Integrity | Protection of Boot Firmware
		Provenance Tracking	• SI-14(1) Non-Persistence | Refresh from Trusted Sources
		Behavior Validation	• AC-2(12) Account Management | Account Monitoring for Atypical Usage • IR-4(13) Incident Handling | Behavior Analysis • SC-36(1) Distributed Processing and Storage | Polling Techniques • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis • SI-4(4) System Monitoring | Inbound and Outbound Communications Traffic • SI-4(13) System Monitoring | Analyze Traffic and Event Patterns

3.9 CSA-09

CSA-09 – **Recover System Capabilities** – After a cyber-event, the system shall be capable of being restored to a known good configuration from a trusted source; at a minimum, restored to partial mission capability, between mission cycles or within xx hours [specified by sponsor], to fight another day. System recovery shall prioritize cyber operational resiliency functions [specified by sponsor]. [1], [2], and [10]

Table 10. Cyber Resiliency Constructs Supporting CSA-09

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
CR Strategic Design Principle: Support agility and architect for adaptability			
Plan and manage diversity	Diversity	Architectural Diversity	• AU-9(7) Protection of Audit Information | Store on Component with Different Operating System • CP-11 Alternate Communications Protocols • CP-13 Alternative Security Mechanisms • SC-29 Heterogeneity • SC-29(1) Heterogeneity | Virtualization Techniques
		Design Diversity	• CP-11 Alternate Communications Protocols • CP-13 Alternative Security Mechanisms

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
		Path Diversity	• AC-7(4) Unsuccessful Logon Attempts | Use of Alternate Authentication Factor • SC-37 Out-Of-Band Channels • SC-47 Alternate Communication Paths
Maintain redundancy	Redundancy	Protected Backup and Restore	• CP-9 System Backup • CP-9(8) System Backup | Cryptographic Protection
		Surplus Capacity	• SC-5(2) Denial of Service Protection | Capacity, Bandwidth, and Redundancy
		Replication	• CP-9(6) System Backup | Redundant Secondary System • PE-9(1) Power Equipment and Cabling | Redundant Cabling • PE-11(1) Emergency Power | Alternate Power Supply – Minimal Operational Capability • PE-11(2) Emergency Power | Alternate Power Supply – Self-Contained • PE-17 Alternate Work Site • SC-36 Distributed Processing and Storage
Manage resources (risk-) adaptively	Adaptive Response	Dynamic Reconfiguration	• AC-4(3) Information Flow Enforcement | Dynamic Information Flow Control • CP-2(5) Contingency Plan | Continue Missions and Business Functions • IR-4(2) Incident Handling | Dynamic Reconfiguration • IR-4(3) Incident Handling | Continuity of Operations • IR-4(9) Incident Handling | Dynamic Response Capability • IR-4(11) Incident Handling | Integrated Incident Response Team • SC-7(20) Boundary Protection | Dynamic Isolation and Segregation
		Adaptive Management	• AC-4(3) Information Flow Enforcement | Dynamic Information Flow Control • CP-2(5) Contingency Plan | Continue Missions and Business Functions • CP-12 Safe Mode • CP-13 Alternative Security Mechanisms • IA-10 Adaptive Authentication • IR-4(3) Incident Handling | Continuity of Operations • IR-4(11) Incident Handling | Integrated Incident Response Team • PE-6(2) Monitoring Physical Access | Automated Intrusion Recognition and Responses • SI-4(7) System Monitoring | Automated Response to Suspicious Events • SI-7(5) Software, Firmware, and Information Integrity | Automated Response to Integrity Violations
CR Strategic Design Principle: Assume compromised resources			
Contain and exclude behaviors	Privilege Restriction	Trust-Based Privilege Management	• AC-6(4) Least Privilege| Separate Processing Domains • AU-9(6) Protection of Audit Information| Read-Only Access
		Attribute-Based Usage Restriction	• AU-9(6) Protection of Audit Information| Read-Only Access
	Segmentation	Predefined Segmentation	• AU-9(2) Protection of Audit Information | Store on Separate Physical Systems and Components • IR-4(12) Incident Handling | Malicious Code and Forensic Analysis • SC-3 Security Function Isolation • SC-3(2) Security Function Isolation | Access and Flow Control Functions • SC-7 Boundary Protection • SC-7(13) Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components • SC-7(22) Boundary Protection | Separate Subnets for Connecting to Different Security Domains • SC-44 Detonation Chambers

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
		Dynamic Segmentation and Isolation	• SC-7(20) Boundary Protection | Dynamic Isolation and Segregation • SC-35 External Malicious Code Identification
Layer defenses and partition resources	Coordinated Protection	Orchestration	• IR-4(3) Incident Handling | Continuity of Operations • IR-4(11) Incident Handling | Integrated Incident Response Team • PE-6(2) Monitoring Physical Access | Automated Intrusion Recognition and Responses • SA-17(8) Developer Security Architecture and Design | Orchestration
	Segmentation	Predefined Segmentation	• AU-9(2) Protection of Audit Information | Store on Separate Physical Systems and Components • IR-4(12) Incident Handling | Malicious Code and Forensic Analysis • SC-3 Security Function Isolation • SC-3(2) Security Function Isolation | Access and Flow Control Functions • SC-7 Boundary Protection • SC-7(13) Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components • SC-7(22) Boundary Protection | Separate Subnets for Connecting to Different Security Domains • SC-44 Detonation Chambers
		Dynamic Segmentation and Isolation	• SC-7(20) Boundary Protection | Dynamic Isolation and Segregation • SC-35 External Malicious Code Identification
Determine ongoing trustworthiness	Substantiated Integrity	Integrity Checks	• AU-9(6) Protection of Audit Information | Read-Only Access • CM-14 Signed Components • SC-34 Non-Modifiable Executable Programs • SC-34(2) Non-Modifiable Executable Programs | Integrity Protection on Read-Only Media • SI-7 Software, Firmware, and Information Integrity • SI-7(1) Software, Firmware, and Information Integrity | Integrity Checks • SI-7(5) Software, Firmware, and Information Integrity | Automated Response to Integrity Violations • SI-7(6) Software, Firmware, and Information Integrity | Cryptographic Protection • SI-7(7) Software, Firmware, and Information Integrity | Integration of Detection and Response • SR-9 Tamper Resistance and Detection
		Provenance Tracking	• SI-14(1) Non-Persistence | Refresh from Trusted Sources
		Behavior Validation	• SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis • SI-4(4) System Monitoring | Inbound and Outbound Communications Traffic • SI-4(13) System Monitoring | Analyze Traffic and Event Patterns
CR Strategic Design Principle: Expect adversaries to evolve			
Make resources location-versatile	Dynamic Positioning	Functional Relocation of Sensors	• IR-4(2) Incident Handling | Dynamic Reconfiguration • SC-48 Sensor Relocation • SC-48(1) Sensor Relocation | Dynamic Relocation of Sensors or Monitoring Capabilities
		Functional Relocation of Cyber Resources	• SC-30(3) Concealment and Misdirection | Change Processing and Storage Locations • SC-36 Distributed Processing and Storage
		Asset Mobility	• SC-36 Distributed Processing and Storage
		Distributed Functionality	• SC-36 Distributed Processing and Storage

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
Leverage health and status data	Analytic Monitoring	Monitoring and Damage Assessment	• AU-6 Audit Record Review, Analysis, and Reporting • AU-6(8) Audit Record Review, Analysis, And Reporting | Full Text Analysis of Privileged Commands • CM-8(3) System Component Inventory | Automated Unauthorized Component Detection • IR-5 Incident Monitoring • PM-31 Continuous Monitoring Strategy • SC-7(10) Boundary Protection | Prevent Exfiltration • SC-26 Decoys • SC-35 External Malicious Code Identification • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis • SI-4(4) System Monitoring | Inbound and Outbound Communications Traffic • SI-4(7) System Monitoring | Automated Response to Suspicious Events • SI-4(18) System Monitoring | Analyze Traffic and Covert Exfiltration • SI-7(7) Software, Firmware, and Information Integrity | Integration of Detection and Response
		Sensor Fusion and Analysis	• AU-6(3) Audit Record Review, Analysis, and Reporting | Correlate Audit Repositories • AU-6(5) Audit Record Review, Analysis, and Reporting | Integrated Analysis of Audit Records • AU-6(6) Audit Record Review, Analysis, and Reporting | Correlation with Physical Monitoring • AU-6(9) Audit Record Review, Analysis, And Reporting | Correlation with Information from Nontechnical Sources • PM-31 Continuous Monitoring Strategy • RA-5(8) Vulnerability Monitoring and Scanning | Review Historic Audit Logs • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis • SI-4(17) System Monitoring | Integrated Situational Awareness • SI-4(24) System Monitoring | Indicators of Compromise
		Forensic and Behavioral Analysis	• IR-4(11) Incident Handling | Integrated Incident Response Team • IR-4(12) Incident Handling | Malicious Code and Forensic Analysis • IR-5 Incident Monitoring • SC-26 Decoys • SC-35 External Malicious Code Identification • SC-44 Detonation Chambers • SI-3(10) Malicious Code Protection | Malicious Code Analysis
	Contextual Awareness	Dynamic Resource Awareness	• SI-4(17) System Monitoring | Integrated Situational Awareness
		Dynamic Threat Awareness	• PM-16 Threat Awareness Program • PM-16(1) Threat Awareness Program | Automated Means for Sharing Threat Intelligence
		Mission Dependency and Status Visualization	• SI-4(1) System Monitoring | System-Wide Intrusion Detection System • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis
Maintain situational awareness	Contextual Awareness	Dynamic Resource Awareness	• SI-4(17) System Monitoring | Integrated Situational Awareness
		Dynamic Threat Awareness	• PM-16 Threat Awareness Program • PM-16(1) Threat Awareness Program | Automated Means for Sharing Threat Intelligence

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
		Mission Dependency and Status Visualization	• SI-4(1) System Monitoring | System-Wide Intrusion Detection System • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis

3.10 CSA-10

CSA-10: Actively Manage System's Configurations to Achieve and Maintain an Operationally-relevant Cyber Risk Posture: Throughout a system's lifecycle and within one standard mission cycle of xx hours [specified by sponsor] of identification of a drop in cyber risk posture below its commensurate CSRC level, the system shall have a configuration management process supported by automated capabilities and technology refresh options, to achieve and continuously maintain an objectively assessed and operationally-relevant risk posture. The process shall include inputs from operators, defenders and intel analysts to continuously assess changes in adversary threat and include a machine readable Bill of Materials (BOM) of the system's GOTS/COTS HW, SW, FW and open source modules for a supply chain risk assessment prior to each milestone decision and supported release. The process shall determine the sufficiency of system cyber survivability and support a DevOps framework to prioritize vulnerability mitigation and remediation in the system and connected infrastructure with greatest mission risks. (note: drives CDRLs). [1] [2] [5]

Table 11. Cyber Resiliency Constructs Supporting CSA-10

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
CR Strategic Design Principle: Focus on common critical assets			
Contain and exclude behaviors	Privilege Restriction	Trust-Based Privilege Management	• AC-3(2) Access Enforcement| Dual Authorization • AC-6(10) Least Privilege| Prohibit Non-Privileged Users from Executing Privileged Functions • CM-5(4) Access Restrictions for Change| Dual Authorization • CP-9(7) System Backup| Dual Authorization
		Attribute-Based Usage Restriction	• AC-3(12) Access Enforcement | Assert and Enforce Application Access • AC-3(13) Access Enforcement | Dynamic Information Flow control • AC-6 Least Privilege • AC-6(1) Least Privilege | Authorize Access to Security Functions • AC-6(8) Least Privilege | Privilege Levels for Code Execution • AC-6(10) Least Privilege| Prohibit Non-Privileged Users from Executing Privileged Functions • RA-5(5) Vulnerability Monitoring and Scanning | Privileged Access
		Dynamic Privileges	• AC-2(6) Account Management | Dynamic Privilege Management • AC-2(8) Account Management | Dynamic Account Management

[5] [Prior wording] **Actively Manage System Configurations to Counter Vulnerabilities at Tactically Relevant Speeds**: Throughout the system's lifecycle and within one standard mission cycle of specified number of hours of notification for operational systems and a specified number of days for systems in development (specified by sponsor), the system shall have a configuration management process supported by automated capabilities to maintain a defined cybersecurity baseline, by authenticating, approving, deploying and verifying the success of cybersecurity configuration changes (including patches and software updates) to mitigate high priority threats on local and remote components, as well as validate that cybersecurity baselines have not been altered. [10]

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
			• AC-6(8) Least Privilege | Privilege Levels for Code Execution • IA-10 Adaptive Authentication
	Segmentation	Predefined Segmentation	• IR-4(12) Incident Handling | Malicious Code and Forensic Analysis • SC-7 Boundary Protection • SC-7(13) Boundary Protection | Isolation of Security Tools, Mechanisms, and Support Components • SC-7(21) Boundary Protection | Isolation of System Components • SC-7(22) Boundary Protection | Separate Subnets for Connecting to Different Security Domains • SC-32 System Partitioning • SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions • SC-39 Process Isolation • SC-39(1) Process Isolation | Hardware Separation • SC-39(2) Process Isolation | Separation Execution Domains Per Thread • SC-44 Detonation Chambers • SC-49 Hardware-Enforced Separation and Policy Enforcement • SC-50 Software-Enforced Separation and Policy Enforcement
		Dynamic Segmentation and Isolation	• SC-7(20) Boundary Protection | Dynamic Isolation and Segregation • SC-18(5) Mobile Code | Allow Execution Only in Confined Environments • SC-32(1) System Partitioning | Separate Physical Domains for Privileged Functions • SC-35 External Malicious Code Identification • SC-39 Process Isolation • SC-39(1) Process Isolation | Hardware Separation • SC-39(2) Process Isolation | Separation Execution Domains Per Thread
Plan and manage diversity	Coordinated Protection	Calibrated Defense-in-Depth	• IA-10 Adaptive Authentication
		Orchestration	• CP-2(5) Contingency Plan | Continue Missions and Business Functions • IR-4(3) Incident Handling | Continuity of Operations • IR-4(10) Incident Handling | Supply Chain Coordination • IR-4(11) Incident Handling | Integrated Incident Response Team • PE-6(2) Monitoring Physical Access | Automated Intrusion Recognition and Responses
		Self-Challenge	• CA-8 Penetration Testing • CA-8(1) Penetration Testing | Independent Penetration Testing Agent or Team • CA-8(2) Penetration Testing | Red Team Exercises • CA-8(3) Penetration Testing | Facility Penetration Testing • CP-4(5) Self-Challenge
	Diversity	Architectural Diversity	• CP-8(3) Telecommunications Services | Separation of Primary and Alternate Providers • CP-11 Alternate Communications Protocols • CP-13 Alternative Security Mechanisms • SC-29 Heterogeneity • SC-29(1) Heterogeneity | Virtualization Techniques
		Design Diversity	• CP-11 Alternate Communications Protocols • CP-13 Alternative Security Mechanisms

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
		Path Diversity	• SC-37 Out-Of-Band Channels • SC-47 Alternate Communication Paths
Leverage health and status data	Analytic Monitoring	Monitoring and Damage Assessment	• AC-2(12) Account Management | Account Monitoring for Atypical Usage • PM-31 Continuous Monitoring Strategy • RA-5(5) Vulnerability Monitoring and Scanning | Privileged Access • RA-10 Threat Hunting • SC-26 Decoys • SC-35 External Malicious Code Identification • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis • SI-4(3) System Monitoring | Automated Tool and Mechanism Integration • SI-4(4) System Monitoring | Inbound and Outbound Communications Traffic • SI-4(7) System Monitoring | Automated Response to Suspicious Events • SI-4(11) System Monitoring | Analyze Communications Traffic Anomalies • SI-4(13) System Monitoring | Analyze Traffic and Event Patterns • SI-4(18) System Monitoring | Analyze Traffic and Covert Exfiltration • SI-7(7) Software, Firmware, and Information Integrity | Integration of Detection and Response
		Sensor Fusion and Analysis	• PM-31 Continuous Monitoring Strategy • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis • SI-4(3) System Monitoring | Automated Tool and Mechanism Integration • SI-4(24) System Monitoring | Indicators of Compromise
		Forensic and Behavioral Analysis	• IR-4(11) Incident Handling | Integrated Incident Response Team • IR-4(12) Incident Handling | Malicious Code and Forensic Analysis • SC-26 Decoys • SC-35 External Malicious Code Identification • SC-44 Detonation Chambers • SI-3(10) Malicious Code Protection | Malicious Code Analysis
	Contextual Awareness	Dynamic Threat Awareness	• PM-16 Threat Awareness Program • RA-3(3) Risk Assessment | Dynamic Threat Awareness • RA-10 Threat Hunting
		Mission Dependency and Status Visualization	• CP-2(8) Contingency Plan | Identify Critical Assets • RA-9 Criticality Analysis • SI-4(1) System Monitoring | System-Wide Intrusion Detection System • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis
Manage resources (risk-) adaptively	Adaptive Response	Dynamic Reconfiguration	• AC-2(6) Account Management | Dynamic Privilege Management • AC-2(8) Account Management | Dynamic Account Management • AC-4(3) Information Flow Enforcement | Dynamic Information Flow Control • CP-2(5) Contingency Plan | Continue Missions and Business Functions • IR-4(2) Incident Handling | Dynamic Reconfiguration • IR-4(3) Incident Handling | Continuity of Operations

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
			• IR-4(9) Incident Handling | Dynamic Response Capability • IR-4(11) Incident Handling | Integrated Incident Response Team • SC-7(20) Boundary Protection | Dynamic Isolation and Segregation
		Dynamic Resource Allocation	• AC-2(8) Account Management | Dynamic Account Management • SC-5(2) Denial of Service Protection | Capacity, Bandwidth, and Redundancy
		Adaptive Management	• AC-2(8) Account Management | Dynamic Account Management • AC-4(3) Information Flow Enforcement | Dynamic Information Flow Control • CP-2(5) Contingency Plan | Continue Missions and Business Functions • CP-12 Safe Mode • CP-13 Alternative Security Mechanisms • IA-10 Adaptive Authentication • IR-4(3) Incident Handling | Continuity of Operations • IR-4(11) Incident Handling | Integrated Incident Response Team • PE-6(2) Monitoring Physical Access | Automated Intrusion Recognition and Responses • RA-3(3) Risk Assessment | Dynamic Threat Awareness • SI-4(3) System Monitoring | Automated Tool and Mechanism Integration • SI-4(7) System Monitoring | Automated Response to Suspicious Events • SI-7(5) Software, Firmware, and Information Integrity | Automated Response to Integrity Violations
Determine ongoing trustworthiness	Substantiated Integrity	Integrity Checks	• CM-14 Signed Components • SI-7 Software, Firmware, and Information Integrity • SI-7(5) Software, Firmware, and Information Integrity | Automated Response to Integrity Violations • SI-7(7) Software, Firmware, and Information Integrity | Integration of Detection and Response • SI-7(12) Software, Firmware, and Information Integrity | Integrity Verification • SR-4(3) Provenance | Validate as Genuine and Not Altered • SR-9 Tamper Resistance and Detection
		Provenance Tracking	• CM-14 Signed Components • SI-7(15) Software, Firmware, And Information Integrity | Code Authentication • SI-14(1) Non-Persistence | Refresh from Trusted Sources • SR-4 Provenance • SR-4(3) Provenance | Validate as Genuine and Not Altered • SR-5 Acquisition Strategies, Tools, And Methods
		Behavior Validation	• AC-2(12) Account Management | Account Monitoring for Atypical Usage • SC-36(1) Distributed Processing and Storage | Polling Techniques • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis • SI-4(4) System Monitoring | Inbound and Outbound Communications Traffic • SI-4(13) System Monitoring | Analyze Traffic and Event Patterns
CR Strategic Design Principle: Expect adversaries to evolve.			
	Contextual Awareness	Dynamic Threat Awareness	• PM-16 Threat Awareness Program • RA-3(3) Risk Assessment | Dynamic Threat Awareness • RA-10 Threat Hunting

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
Maintain situational awareness		Mission Dependency and Status Visualization	• CP-2(8) Contingency Plan | Identify Critical Assets • RA-9 Criticality Analysis • SI-4(1) System Monitoring | System-Wide Intrusion Detection System • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis
Leverage health and status data	Analytic Monitoring	Monitoring and Damage Assessment	• AC-2(12) Account Management | Account Monitoring for Atypical Usage • PM-31 Continuous Monitoring Strategy • RA-5(5) Vulnerability Monitoring and Scanning | Privileged Access • RA-10 Threat Hunting • SC-26 Decoys • SC-35 External Malicious Code Identification • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis • SI-4(3) System Monitoring | Automated Tool and Mechanism Integration • SI-4(4) System Monitoring | Inbound and Outbound Communications Traffic • SI-4(7) System Monitoring | Automated Response to Suspicious Events • SI-4(11) System Monitoring | Analyze Communications Traffic Anomalies • SI-4(13) System Monitoring | Analyze Traffic and Event Patterns • SI-4(18) System Monitoring | Analyze Traffic and Covert Exfiltration • SI-7(7) Software, Firmware, and Information Integrity | Integration of Detection and Response
		Sensor Fusion and Analysis	• PM-31 Continuous Monitoring Strategy • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis • SI-4(3) System Monitoring | Automated Tool and Mechanism Integration • SI-4(24) System Monitoring | Indicators of Compromise
		Forensic and Behavioral Analysis	• IR-4(11) Incident Handling | Integrated Incident Response Team • IR-4(12) Incident Handling | Malicious Code and Forensic Analysis • SC-26 Decoys • SC-35 External Malicious Code Identification • SC-44 Detonation Chambers • SI-3(10) Malicious Code Protection | Malicious Code Analysis
	Contextual Awareness	Dynamic Threat Awareness	• PM-16 Threat Awareness Program • RA-3(3) Risk Assessment | Dynamic Threat Awareness • RA-10 Threat Hunting
		Mission Dependency and Status Visualization	• CP-2(8) Contingency Plan | Identify Critical Assets • RA-9 Criticality Analysis • SI-4(1) System Monitoring | System-Wide Intrusion Detection System • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis
Manage resources (risk-) adaptively	Adaptive Response	Dynamic Reconfiguration	• AC-2(6) Account Management | Dynamic Privilege Management • AC-2(8) Account Management | Dynamic Account Management • AC-4(3) Information Flow Enforcement | Dynamic Information Flow Control

CR Structural Design Principle	CR Techniques	CR Approach	NIST SP 800-53 R5 controls
			• CP-2(5) Contingency Plan | Continue Missions and Business Functions • IR-4(2) Incident Handling | Dynamic Reconfiguration • IR-4(3) Incident Handling | Continuity of Operations • IR-4(9) Incident Handling | Dynamic Response Capability • IR-4(11) Incident Handling | Integrated Incident Response Team • SC-7(20) Boundary Protection | Dynamic Isolation and Segregation
		Dynamic Resource Allocation	• AC-2(8) Account Management | Dynamic Account Management • SC-5(2) Denial of Service Protection | Capacity, Bandwidth, and Redundancy
		Adaptive Management	• AC-2(8) Account Management | Dynamic Account Management • AC-4(3) Information Flow Enforcement | Dynamic Information Flow Control • CP-2(5) Contingency Plan | Continue Missions and Business Functions • CP-12 Safe Mode • CP-13 Alternative Security Mechanisms • IA-10 Adaptive Authentication • IR-4(3) Incident Handling | Continuity of Operations • IR-4(11) Incident Handling | Integrated Incident Response Team • PE-6(2) Monitoring Physical Access | Automated Intrusion Recognition and Responses • RA-3(3) Risk Assessment | Dynamic Threat Awareness • SI-4(3) System Monitoring | Automated Tool and Mechanism Integration • SI-4(7) System Monitoring | Automated Response to Suspicious Events • SI-7(5) Software, Firmware, and Information Integrity | Automated Response to Integrity Violations
Determine ongoing trustworthiness	Substantiated Integrity	Integrity Checks	• CM-14 Signed Components • SI-7 Software, Firmware, and Information Integrity • SI-7(5) Software, Firmware, and Information Integrity | Automated Response to Integrity Violations • SI-7(7) Software, Firmware, and Information Integrity | Integration of Detection and Response • SI-7(12) Software, Firmware, and Information Integrity | Integrity Verification • SR-4(3) Provenance | Validate as Genuine and Not Altered • SR-9 Tamper Resistance and Detection
		Provenance Tracking	• CM-14 Signed Components • SI-7(15) Software, Firmware, And Information Integrity | Code Authentication • SI-14(1) Non-Persistence | Refresh from Trusted Sources • SR-4 Provenance • SR-4(3) Provenance | Validate as Genuine and Not Altered • SR-5 Acquisition Strategies, Tools, And Methods
		Behavior Validation	• AC-2(12) Account Management | Account Monitoring for Atypical Usage • SC-36(1) Distributed Processing and Storage | Polling Techniques • SI-4(2) System Monitoring | Automated Tools and Mechanisms for Real-Time Analysis • SI-4(4) System Monitoring | Inbound and Outbound Communications Traffic • SI-4(13) System Monitoring | Analyze Traffic and Event Patterns

4 Conclusion

This report provides an initial analysis of how cyber resiliency (design principles, techniques, approaches and controls) may be used to support the implementation of the Cyber Survivability Attributes defined in the CSEIG. The AFRL CSA Tool has incorporated the identification of cyber resiliency controls which support CSAs, as captured in the tables in Section 3. Mapping activities such as this reconcile the authoritative sources – showing how the language of the CSEIG may be mapped to the language in 800-160 V2 using the security controls. The NIST SP 800-53 R5 controls can be used as the "lingua franca". Although the mapping activities were a collaborative effort between MITRE, AFRL, and Joint Staff/J6 personnel, this mapping only incorporates limited community feedback. The mappings will mature over time with more feedback based on use in specific contexts.

The work documented here was deliberately limited in scope, focusing on the exemplar language and on the techniques *required* to apply the identified cyber resiliency design principles. This report thus does not identify all techniques, approaches, or controls which could improve CSA effectiveness, or which could enable active cyber defense. In particular, Deception and Unpredictability are increasingly powerful techniques for cyber defenders. While Deception is not a required technique in the methodology applied, the Obfuscation approach within Deception was identified as useful in supporting some of the CSAs; Disinformation could significantly support CSA-04. Similarly, the Evolvability approach to Realignment could significantly support CSA-10. Likewise, both Temporal Unpredictability and Contextual Unpredictability could significantly support CSA-03 and CSA-04. Further analysis is needed.

The work documented here is subject to the caveats described in Section 2.3: it is based on exemplar language, restricted to cyber resiliency controls, does not include related controls, is limited to techniques required by the identified design principles, and assumes controls are implemented (and implementations are used) to apply the identified design principles and support the identified CSAs. As the cyber resiliency mappings are applied to the CSAs in various contexts (i.e., as the exemplar language is tailored for a specific system, and refined over the course of the SDLC), systems engineers can expect to find other cyber resiliency techniques, approaches, and controls that are useful in supporting the implementation of specific CSAs. The mappings presented in this report are intended to serve as a starting point; a range of more specific examples (e.g., covering tactical, mission planning, and infrastructure systems) could be developed to provide more nuanced guidance.

5 References

[1] Joint Staff/J6, *Cyber Survivability Endorsement (CSE) Implementation Guide, Version 3.0 (cleared for public release),* Joint Staff J6, Deputy Director for Information Warfare Requirements Division, July 2022.

[2] S. Pitcher and T. Andress, "Cyber Survivability for Future and Legacy DoD Weapon Systems," 10 June 2021. [Online]. Available: https://www.ndia.org/-/media/sites/ndia/divisions/systems-engineering/se---june-2021-meeting/cse-support-to-future-and-legacy-dod-systems-10-jun-2021-for-ndia.ashx.

[3] DoD CIO, "DoD Instruction 8510.01, Risk Management Framework for DoD Systems," 19 July 2022. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf.

[4] Joint Task Force, "NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations," 23 September 2020. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf.

[5] NIST, "NIST SP 800-160 Volume 2, Developing Cyber Resilient Systems: A Systems Security Engineering Approach," 27 November 2019. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2.pdf.

[6] NIST, "NIST SP 800-160 Vol. 2 Rev. 1 (DRAFT), Developing Cyber Resilient Systems: A Systems Security Engineering Approach," August 2021. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1-draft.pdf.

[7] D. Bodeau, R. Graubart and E. Laderman, "Relationships Between Cyber Resiliency Constructs and Cyber Survivability Attributes: Enabling Controls, Requirements, Solutions, and Metrics to Be Defined, MP190668, PR 19-02172-10," September 2019. [Online]. Available: https://www.mitre.org/sites/default/files/2022-09/pr-19-02172-10-cyber-resiliency-constructs-cyber-survivability.pdf.

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

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

[10] S. Pitcher, "New DoD approaches on the Cyber Survivability of Weapon Systems," 25 March 2019. [Online]. Available: http://www.itea.org/wp-content/uploads/2019/03/Pitcher-Steve.pdf. [Accessed 19 August 2020].

[11] D. J. Bodeau, R. D. Graubart, E. Laderman, L. K. Jones and D. Black, "Cyber Resiliency Approaches and Controls to Mitigate Adversary Tactics, Techniques, and Procedures (TTPs): Mapping Cyber Resiliency to the ATT&CK® Framework – Revision 2, MTR200286R2, PR 21-3123," December 2021. [Online]. Available: https://www.mitre.org/sites/default/files/publications/pr-21-3123-cyber-resiliency-approaches-control-mitigate-adversary-tactics-techniques-procedures-ttps-mapping-cyber-resiliency-attack-framework-revision-2.pdf.

[12] Joint Task Force Transformative Initiative, "NIST SP 800-53 Revision 4 Security and Privacy Controls for Federal Information Systems and Organizations," April 2013. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[13] The Committee on National Security Systems (CNSS), *CNSSI No. 1253, Security Categorization and Control Selection for National Security Systems,* 2014.

[14] The Committee on National Security Systems (CNSS), "CNSSI 1253, Categorization and Control Selection for National Security Systems," 29 July 2022. [Online]. Available: https://www.cnss.gov/CNSS/openDoc.cfm?h9YgIUkcbMNnyyvTAitdRQ==.

[15] D. Bodeau and R. Graubart, "Cyber Resiliency Assessment: Enabaling Architectural Improvement(MTR 120407, PR12-3795)," May 2013. [Online]. Available: http://www.mitre.org/sites/default/files/pdf/12-3795.pdf.

[16] T. Gregg and M. Long, "Framework for Improving Critical Infrastructure Cybersecurity/ATT&CK™ Mapping, PR 19-3442," The MITRE Corporation, McLean, VA, 2019.

[17] J. Baker and T. Bergeron, "Security Control Mappings: A Bridge to Threat-Informed Defense," MITRE-Engenuity, 15 December 2020. [Online]. Available: https://medium.com/mitre-engenuity/security-control-mappings-a-bridge-to-threat-informed-defense-2e42a074f64a.

[18] DoD CIO, "DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT) (Incorporating Change 3, December 29, 2020)," 12 March 2014. [Online]. Available: https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/851001p.pdf.

[19] Joint Chiefs of Staff, "Cyber Survivability Endorsement Implementation Guide, Version 2.0," 2020 "not in the public domain".

Appendix A Cyber Resiliency Constructs

The tables in this appendix are adapted from Appendix F of NIST SP 800-160 Vol. 2 R1, presented in the order the cyber resiliency constructs were used in the analysis process described in Section 2 above: strategic design principles, structural design principles, techniques, and implementation approaches. See Appendix D of [6] for the complete definition and examples of technologies and practices for each approach, and for guidance on where in a notional layered architecture each approach could be used. To facilitate use in the context of cyber survivability of weapon systems and defense critical infrastructure systems, annotations in *italics* are added to the material from NIST SP 800-160 Vol. 2 R1.

Table 12. Strategic Cyber Resiliency Design Principles

STRATEGIC DESIGN PRINCIPLES	KEY IDEAS and *CONCERNS FOR WEAPON SYSTEMS AND CRITICAL INFRASTRUCTURES*	SUPPORTED CSAs
Focus on common critical assets.	Limited organizational and programmatic resources need to be applied where they can provide the greatest benefit. This results in a strategy of focusing first on assets which are both critical and common, then on those which are either critical or common. *Common critical assets are a focus during cyber events because their performance can have the highest impacts and decisions about who gets priority access to resources must be made addressing cyber events. Asset criticality can depend on the defense condition, mission phase, or set of mission activities being executed at a given time.*	**CSA-03, CSA-04, CSA-05, CSA-07, CSA-08, CSA-10**
Support agility and architect for adaptability.	Not only does the threat landscape change as adversaries evolve, so do technologies and the ways in which individuals and organizations use them. Both agility and adaptability are integral to the risk management strategy in response to the risk framing assumption that unforeseen changes will occur in the threat, technical, and operational environment through a system's lifespan. *Agility and adaptability increase options for operation in a compromised environment and for recovery.*	**CSA-02, CSA-08, CSA-09**
Reduce attack surfaces.	A large attack surface is difficult to defend, requiring ongoing effort to monitor, analyze, and respond to anomalies. Reducing attack surfaces reduces ongoing protection scope costs and makes the adversary concentrate efforts on a small set of locations, resources, or environments that can be more effectively monitored and defended. *Attack surfaces can be reduced, hardened, and monitored at multiple points in the SDLC, including via supply chain risk management.*	**CSA-02, CSA-06**
Assume compromised resources.	Systems and system components, ranging from chips to software modules to running services, can be compromised for extended periods without detection. In fact, some compromises may never be detected. Systems must remain capable of meeting performance and quality requirements, nonetheless. *Compromised resources can interfere with safe and secure recovery.*	**CSA-01, CSA-03, CSA-05, CSA-06, CSA-09**
Expect adversaries to evolve.	Advanced cyber adversaries invest time, effort, and intelligence-gathering to improve existing and develop new TTPs. Adversaries evolve in response to opportunities offered by new technologies or uses of technology, as well as to the knowledge they gain about defender TTPs. In (increasingly short) time, the tools developed by advanced adversaries become available to less sophisticated adversaries. Therefore, systems and missions need to be resilient in the face of unexpected attacks. *Cyber tabletop exercises (CTTX) provide a vital analysis method.*	**CSA-06, CSA-08, CSA-09, CSA-10**

Table 13. Structural Cyber Resiliency Design Principles

STRUCTURAL DESIGN PRINCIPLES	KEY IDEAS	SUPPORTED CSAs
Limit the need for trust.	Limiting the number of system elements that need to be trusted (or the length of time an element needs to be trusted) reduces the level of effort needed for assurance, as well as for ongoing protection and monitoring.	**CSA-03, CSA-05, CSA-06**
Control visibility and use.	Controlling what can be discovered, observed, and used increases the effort needed by an adversary seeking to expand its foothold in or increase its impacts on systems containing cyber resources.	**CSA-01, CSA-02, CSA-03, CSA-04, CSA-08**
Contain and exclude behaviors.	Limiting what can be done and where actions can be taken reduces the possibility or extent of the spread of compromises or disruptions across components or services.	**CSA-04, CSA-06, CSA-08, CSA-09, CSA-10**
Layer defenses and partition resources.	The combination of defense-in-depth and partitioning increases the effort required by an adversary to overcome multiple defenses.	**CSA-03, CSA-04, CSA-05, CSA-06 CSA-09**
Plan and manage diversity.	Diversity is a well-established resilience technique, removing single points of attack or failure. However, architectures and designs should take cost and manageability into consideration to avoid introducing new risks.	**CSA-05, CSA-08, CSA-09, CSA-10**
Maintain redundancy.	Redundancy is key to many resilience strategies but can degrade over time as configurations are updated or connectivity changes.	**CSA-03, CSA-05, CSA-08, CSA-09**
Make resources location-versatile.	A resource bound to a single location (e.g., a service running only on a single hardware component, a database located in a single datacenter) can become a single point of failure and thus a high value target.	**CSA-02, CSA-09**
Leverage health and status data.	Health and status data can be useful in supporting situational awareness, indicating potentially suspicious behaviors, and predicting the need for adaptation to changing operational demands.	**CSA-05, CSA-06, CSA-07, CSA-08, CSA-09, CSA-10**
Maintain situational awareness.	Situational awareness, including awareness of possible performance trends and the emergence of anomalies, informs decisions about cyber courses of action to ensure mission completion.	**CSA-07, CSA-08, CSA-09, CSA-10**
Manage resources (risk-) adaptively.	Risk-adaptive management supports agility, providing supplemental risk mitigation throughout critical operations despite disruptions or outages of components.	**CSA-05, CSA-08, CSA-09, CSA-10**
Maximize transience.	Use of transient system elements minimizes the duration of exposure to adversary activities, while periodically refreshing to a known (secure) state can expunge malware or corrupted data.	**CSA-02, CSA-03, CSA-04, CSA-05**
Determine ongoing trustworthiness.	Periodic or ongoing verification and/or validation of the integrity or correctness of data or software can increase the effort needed by an adversary seeking to modify or fabricate data or functionality. Similarly, periodic or ongoing analysis of the behavior of individual users, system components, and services can increase suspicion, triggering responses such as closer monitoring, more restrictive privileges, or quarantine.	**CSA-01, CSA-03, CSA-04, CSA-06, CSA-08, CSA-09, CSA-10**
Change or disrupt the attack surface.	Disruption of the attack surface can cause the adversary to waste resources, make incorrect assumptions about the system or the defender, or prematurely launch attacks or disclose information.	**CSA-03, CSA-04, CSA-05, CSA-06**
Make the effects of deception and unpredictability user-transparent.	Deception and unpredictability can be highly effective techniques against an adversary, leading the adversary to reveal its presence or TTPs or to waste effort. However, when improperly applied, these techniques can also confuse users.	**CSA-06**

Table 14. Cyber Resiliency Techniques and Approaches

TECHNIQUES	APPROACHES	SUPPORTED CSAs
Adaptive Response Implement agile courses of action to manage risks. *Inform courses of action with situational awareness and predictive analytics for increased agility.* *All approaches can leverage virtualization and are compatible with zero trust architecture (ZTA) and cloud computing strategies. All approaches can also be applied to processes and reporting within a Security Operations Center (SOC), and to the use of deception.*	**Dynamic Reconfiguration** Definition: Make changes to individual systems, system elements, components, or sets of resources to change functionality or behavior without interrupting service. Informal description: Change how resources are – or can be – used. *Reconfiguration needs to be executed without significantly degrading or interrupting service.*	**CSA-05, CSA-08, CSA-09, CSA-10**
	Dynamic Resource Allocation Definition: Change the allocation of resources to tasks or functions without terminating critical functions or processes. Informal description: Change how much of a resource can be used. *Reallocate resources to tasks or functions without terminating critical functions or processes.*	**CSA-05, CSA-08, CSA-10**
	Adaptive Management Definition: Change how mechanisms are used based on changes in the operational environment as well as changes in the threat environment. Informal description: Change in response to change. *Manage how mechanisms can be used based on changes in the operational environment as well as changes in the threat environment.*	**CSA-05, CSA-08, CSA-09, CSA-10**
Analytic Monitoring Monitor and analyze a wide range of properties and behaviors on an ongoing basis and in a coordinated way. *Systems can accumulate vast amounts of monitoring or logging data. Use monitoring data strategically to inform defensive activities.*	**Monitoring and Damage Assessment** Definition: Monitor and analyze behavior and characteristics of components and resources to look for indicators of adversary activity, to look for precursor conditions or indicators of other threat events, and to detect and assess damage from adversity. Informal description: Look for indications that something might be awry and what damage might have occurred. *Leverage Continuous Diagnostics and Monitoring (CDM) and other monitoring capabilities, including those related to health and status (H&S). Integrate with threat hunting and insider threat monitoring.*	**CSA-06, CSA-07, CSA-08, CSA-09, CSA-10**
	Sensor Fusion and Analysis Definition: Fuse and analyze monitoring data and analysis results from different information sources or at different times together with externally provided threat intelligence. Informal description: Put the pieces together – from many different sources. *Consider all possible sources of monitoring information, including CDM, H&S, physical access logs, and insider threat monitoring.*	**CSA-05, CSA-07, CSA-08, CSA-10**
	Forensic and Behavioral Analysis Definition: Analyze indicators and adversary TTPs, including observed behavior as well as malware and other artifacts left behind by adverse events. Informal description: Analyze adversary activities and artifacts to develop understanding and attribution of adversary goals, capabilities, and practices. *Ensure that policies and practices are in place to capture evidence and support analysis.*	**CSA-06, CSA-07 CSA-08, CSA-09, CSA-10**
Contextual Awareness Construct and maintain current representations of the posture of missions or business functions considering threat events and courses of action.	**Dynamic Resource Awareness** Definition: Maintain current information about resources, status of resources, and resource connectivity. Informal description: Maintain awareness of systems' performance and security posture. *Integrate network performance, system performance, and continuous diagnostics as part of situational awareness.*	**CSA-05, CSA-07, CSA-08, CSA-09**

TECHNIQUES	APPROACHES	SUPPORTED CSAs
Maintain cyber situational awareness to support mission continuity.	**Dynamic Threat Awareness** Definition: Maintain current information about threat actors, indicators, and potential, predicted, and observed adverse events. Informal description: Maintain current awareness of threats – observed and anticipated. *Ensure that the organization's Security Operations Center (SOC) ingests cyber threat intelligence.*	**CSA-05, CSA-07, CSA-08, CSA-09, CSA-10**
	Mission Dependency and Status Visualization Definition: Maintain a useful current visualization of the status of missions or business functions, dependencies on resources, and the status of those resources with respect to threats. Informal description: Maintain an up-to-date cyber operational picture. *Maintain an up-to-date dependency map for mission essential or business essential functions. Integrate resource and threat awareness into situational awareness, and enable focused visualization for high value assets and infrastructure services.*	**CSA-05, CSA-07, CSA-08, CSA-09, CSA-10**
Coordinated Protection Ensure that protection mechanisms operate in a coordinated and effective manner. *Lack of coordination introduces fragility and creates exposures to threats.*	**Calibrated Defense-in-Depth** Definition: Provide complementary protective mechanisms at different architectural layers or in different locations, calibrating the strength and number of mechanisms to resource value. Informal description: Don't expect one defense to suffice – but apply layered defenses based on risk. *Avoid creating single points of failure. Do not make the adversary's job easy.*	**CSA-03, CSA-05, CSA-06, CSA-08, CSA-10**
	Consistency Analysis Definition: Determine whether and how protections can be applied in a coordinated, consistent way that minimizes interference, potential cascading failures, or coverage gaps. Informal description: Minimize opportunities for the system's security capabilities to be used incompletely or inconsistently. *Over time, changing access policies for information, allowable uses of capabilities, and dependencies among systems and components can produce fragility and provide adversaries with opportunities.*	**CSA-08**
	Orchestration Definition: Coordinate modifications to and the ongoing behavior of mechanisms and processes at different layers, in different locations, or implemented for different aspects of trustworthiness to avoid causing cascading failures, interference, or coverage gaps. Informal description: Coordinate security capabilities at different layers, and in different systems or components, to avoid coverage gaps or interference. *Orchestrate updates of capabilities and policies – in particular, for identity, credentialing, and access management (ICAM) – across systems. Orchestrate monitoring across architectural layers. Use a cyber playbook to orchestrate incident response efforts.*	**CSA-03, CSA-05, CSA-06, CSA-08, CSA-09, CSA-10**
	Self-Challenge Definition: Affect mission/business processes or system elements adversely in a controlled manner to validate the effectiveness of protections and to enable proactive response and improvement. Informal description: Validate the effectiveness of capabilities and processes in action. *Use tabletop exercises (TTXs), Red Teams, penetration testing, or automated fault injection throughout the system lifecycle and with different scopes.*	**CSA-04, CSA-06, CSA-08, CSA-10**
Deception	**Obfuscation** Definition: Hide, transform, or otherwise make information unintelligible to the adversary.	**CSA-02, CSA-03, CSA-04**

TECHNIQUES	APPROACHES	SUPPORTED CSAs
Mislead, confuse, hide critical assets from, or expose covertly tainted assets to the adversary. *Apply deception strategically, tactically, or both. Ensure that cyber risk governance and SOC operations allow for deception and maintain deception resources. Deception can support analysis and attribution of adversary TTPs, and the development of cyber threat intelligence.*	Informal description: Make information hard for the adversary to find and understand. *Encryption is a key method for obfuscation.*	
	Disinformation Definition: Provide deliberately misleading information to adversaries. Informal description: Lie to adversaries. *Typical forms of disinformation include decoy accounts and decoy credentials.*	**CSA-04**
	Misdirection Definition: Maintain deception resources or environments and direct adversary activities there. Informal description: Direct adversary activities to deception environments or resources. *Commercial products can be used to create and maintain a deception network, but ongoing effort is needed to keep it current, engage with adversaries, and analyze adversary TTPs.*	**[related to active cyber defense, rather than to CSAs]**
	Tainting Definition: Embed covert capabilities in resources. Informal description: Cause what adversaries steal to give them away or otherwise harm them. *Enable exfiltrated data to "phone home."*	**[related to active cyber defense, rather than to CSAs]**
Diversity Use heterogeneity to minimize common mode failures, particularly threat events exploiting common vulnerabilities. *Enterprise systems often include some diversity incidentally, as a result of procurements by different programs or at different times. Poorly managed, this can be costly and create security risks; well managed, it can make an adversary's job harder.* *Due to reliance on common libraries and infrastructures, diversity can be more apparent than real; therefore, analysis is needed to verify the extent of diversity.*	**Architectural Diversity** Definition: Use multiple sets of technical standards, different technologies, and different architectural patterns. Informal description: Use different technical architectures. *An organization can use, for example, both Windows and Linux. An organization's cloud strategy can involve multiple cloud infrastructures.*	**CSA-05, CSA-08, CSA-09, CSA-10**
	Design Diversity Definition: Use different designs within a given architecture to meet the same requirements or provide equivalent functionality. Informal description: Provide multiple ways to meet requirements. *Within the context of a given architecture, parallel design teams can solve the same problem in different ways, thus producing different attack surfaces.*	**CSA-05, CSA-08, CSA-09, CSA-10**
	Synthetic Diversity Definition: Transform implementations of software to produce a variety of instances. Informal description: Use automation to tweak software implementations. *For example, use randomizing compilers or address space layout randomization.*	**CSA-05, CSA-08, CSA-09**
	Information Diversity Definition: Provide information from different sources or transform information in different ways. Informal description: Use multiple sources for the same information. *Use of information from different sources can reveal adversary injection or modification.*	**CSA-08**
	Path Diversity Definition: Provide multiple independent paths for command, control, and communications. Informal description: Do not rely on a single mode of communication. *In particular, ensure alternative lines of communications for incident response and for continuity of an organization's essential functions.*	**CSA-05, CSA-08, CSA-09, CSA-10**
	Supply Chain Diversity Definition: Use multiple independent supply chains for critical components.	**CSA-08**

TECHNIQUES	APPROACHES	SUPPORTED CSAs
	Informal description: Look for ways to avoid relying on a single supply chain. *Determine when and how to use supply chain diversity as part of the organization's supply chain risk management (SCRM) strategy. Note that the use of shared libraries and common components can make supply chain diversity more apparent than real.*	
Dynamic Positioning Distribute and dynamically relocate functionality or system resources. *Use moving target defenses to make an adversary's job harder.*	**Functional Relocation of Sensors** Definition: Relocate sensors or reallocate responsibility for specific sensing tasks to look for indicators of adverse events. Informal description: Keep your eyes moving. *Relocating sensors compensates for blind spots and makes it harder for an adversary to hide.*	**CSA-02, CSA-09**
	Functional Relocation of Cyber Resources Definition: Change the location of cyber resources that provide functionality or information, either by moving the assets or by transferring functional responsibility. Informal description: Keep your cyber resources moving. *Make the adversary's discovery and network mapping efforts go stale quickly.*	**CSA-02, CSA-03, CSA-04, CSA-05, CSA-09**
	Asset Mobility Definition: Securely move physical resources. Informal description: Don't pin your physical resource down. *This approach is applicable to cyber-physical and tactical systems.*	**CSA-02, CSA-03, CSA-04, CSA-05, CSA-09**
	Fragmentation Definition: Partition information and distribute it across multiple components. Informal description: Create an information jigsaw puzzle. *Manage fragmented data to ensure its ongoing quality, minimize its exposure, and minimize performance inefficiencies.*	**CSA-02, CSA-04,**
	Distributed Functionality Definition: Decompose a function or application into smaller functions and distribute those functions across multiple components. Informal description: Use fine-grained control of resource use. *Distributed functionality can be used with micro-segmentation and ZTA.*	**CSA-02, CSA-03, CSA-04, CSA-05, CSA-09**
Non-Persistence Generate and retain resources as needed or for a limited time. *Reduce the attack surface in the temporal dimension, and reduce costs with just-in-time provisioning.*	**Non-Persistent Information** Definition: Refresh information periodically, or generate information on demand, and delete it when no longer needed. Informal description: Limit how long information is exposed. *Determine how temporary "temporary" files are.*	**CSA-02, CSA-04, CSA-06**
	Non-Persistent Services Definition: Refresh services periodically, or generate services on demand and terminate services when no longer needed. Informal description: Don't let a service run indefinitely – it may have been compromised while running. *Instantiating services on demand and expunging them when inactive can be a performance management strategy as well.*	**CSA-02, CSA-03, CSA-05, CSA-06**
	Non-Persistent Connectivity Definition: Establish connections on demand, and terminate connections when no longer needed. Informal description: Don't leave a communications line open. *Leverage software-defined networking (SDN), particularly in a ZTA.*	**CSA-02, CSA-03, CSA-05, CSA-06**
Privilege Restriction Restrict privileges based on attributes of users and system elements as well as on environmental factors.	**Trust-Based Privilege Management** Definition: Define, assign, and maintain privileges based on established trust criteria consistent with principles of least privilege. Informal description: Apply principles of least privilege. *Separate roles and responsibilities, use dual authorization.*	**CSA-01, CSA-03, CSA-04, CSA-06, CSA-08, CSA-09, CSA-10**

TECHNIQUES	APPROACHES	SUPPORTED CSAs
Apply existing capabilities more stringently, and integrate ZT technologies.	**Attribute-Based Usage Restriction** Definition: Define, assign, maintain, and apply usage restrictions on cyber resources based on the criticality of missions or business functions and other attributes (e.g., data sensitivity). Informal description: Restrict use narrowly. *Avoid treating a system or an application as a Swiss Army knife.*	**CSA-01, CSA-03, CSA-04, CSA-06, CSA-08, CSA-09, CSA-10**
	Dynamic Privileges Definition: Elevate or decrease privileges assigned to a user, process, or service based on transient or contextual factors. Informal description: Make privileges context-sensitive. *Make access and usage decisions based on the current state and recent history.*	**CSA-01, CSA-03, CSA-04, CSA-06, CSA-08, CSA-10**
Realignment Structure systems and resource uses to meet mission or business function needs, to reduce current and anticipated risks, and to accommodate evolution of the technical, operational, and threat environments. *Look for restructuring opportunities related to new systems and programs, as well as planned upgrades to existing systems.*	**Purposing** Definition: Ensure cyber resources are used consistently with mission or business function purposes and approved uses, thereby avoiding unnecessary sharing and complexity. Informal description: Ensure resources are used consistently with mission or business function purposes and approved uses. *Avoid "mission creep," which can increase a system's attack surface.*	**CSA-06**
	Offloading Definition: Offload supportive but non-essential functions to other systems or to an external provider that is better able to perform the functions securely. Informal description: Offload functions when an external provider can do a better job. *Offloading reduces the attack surface and motivates ongoing consideration of what's essential.*	**CSA-03, CSA-05, CSA-06**
	Restriction Definition: Remove or disable unneeded functionality or connectivity. Informal description: Lock capabilities down. *Lock it down, even though that reduces agility and leaves some capabilities unused.*	**CSA-05, CSA-06**
	Replacement Definition: Replace low-assurance or poorly understood components with more trustworthy ones. Informal description: Replace what can't be trusted. *Some components are best simply discarded, particularly in light of supply chain risks. However, the decommissioning and replacement processes need to be secure.*	**CSA-06**
	Specialization Definition: Modify the design of, augment, or configure critical cyber resources uniquely for the mission or business function to improve trustworthiness. Informal description: Build special-purpose components or develop "special sauce." *Prevent the adversary from being able to mirror your system.*	**CSA-06**
	Evolvability Definition: Provide mechanisms and structure resources to enable the system to be maintained, modified, extended, or used in new ways without increasing security or mission risk. Informal description: Don't commit to an unchanging architecture. *Expect a broader range of "plug and play" capabilities over time.*	**[related to CSA-10]**
Redundancy Provide multiple protected instances of critical resources. *Redundancy is integral to system resilience, but it must be*	**Protected Backup and Restore** Definition: Back up information and software (including configuration data and virtualized resources) in a way that protects its confidentiality, integrity, and authenticity, and enable safe and secure restoration in case of disruption or corruption.	**CSA-05, CSA-08, CSA-09**

TECHNIQUES	APPROACHES	SUPPORTED CSAs
managed carefully to avoid redundant vulnerabilities and an increased attack surface.	Informal description: Back up resources securely, and defend the restore process from adversary exploitation. *Keep in mind that transitions are often periods of exposure, and backups can be compromised.*	
	Surplus Capacity Definition: Maintain extra capacity for information storage, processing, or communications. Informal description: Don't skimp on resources – provide surge capacity. *Where possible, use diverse resources to provide surplus capacity.*	**CSA-03, CSA-05, CSA-08, CSA-09**
	Replication Definition: Duplicate hardware, information, backups, or functionality in multiple locations and keep them synchronized. Informal description: Replicate capabilities in multiple locations and keep them synchronized. *Where possible, replicate capabilities using diverse resources.*	**CSA-03, CSA-05, CSA-08, CSA-09**
Segmentation Define and separate system elements based on criticality and trustworthiness. *Reduce the adversary's scope for lateral movement or command and control (C2).*	**Predefined Segmentation** Definition: Define enclaves, segments, micro-segments, or other restricted types of resource sets based on criticality and trustworthiness so that they can be protected separately and, if necessary, isolated. Informal description: Define enclaves, segments, or micro-segments to protect them separately. *Predefined enclaves and micro-segmentation facilitate risk-calibrated use of other security and cyber resiliency techniques.*	**CSA-01, CSA-02, CSA-03, CSA-04, CSA-05, CSA-06, CSA-08, CSA-09, CSA-10**
	Dynamic Segmentation and Isolation Definition: Change the configuration of enclaves or protected segments, or isolate resources while minimizing operational disruption. Informal description: Isolate resources dynamically to reduce transient risks. *Consider software-defined networking (SDN) and network function virtualization (NFV), consistent with ZT principles, particularly for high value assets.*	**CSA-01, CSA-02, CSA-05, CSA-06, CSA-08, CSA-09, CSA-10**
Substantiated Integrity Ascertain whether critical system elements have been corrupted. *Verify that you actually have what you think you have.*	**Integrity Checks** Definition: Apply and validate checks of the integrity or quality of information, components, or services, to guard against surreptitious modification. Informal description: Check for modifications to data and software. *Integrity checks can be applied to information, metadata, components, or services.*	**CSA-01, CSA-03, CSA-04, CSA-06, CSA-08, CSA-09, CSA-10**
	Provenance Tracking Definition: Identify and track the provenance of data, software, or hardware elements. Informal description: Verify the source of what you depend on. *Make provenance tracking part of SCRM.*	**CSA-03, CSA-06, CSA-08, CSA-09, CSA-10**
	Behavior Validation Definition: Validate the behavior of a system, service, device, or individual user against defined or emergent criteria (e.g., requirements, patterns of prior usage). Informal description: Validate behavior against defined or emergent criteria. *Learn what's normal and what's suspicious. Coordinate with insider threat mitigation.*	**CSA-01, CSA-03, CSA-06, CSA-08, CSA-09, CSA-10**
Unpredictability Make changes randomly or unpredictably.	**Temporal Unpredictability** Informal description: Change behavior or state at times that are determined randomly or by complex functions.	**CSA-02, CSA-05**

TECHNIQUES	APPROACHES	SUPPORTED CSAs
Keep the adversary guessing.	Informal description: Keep the adversary from extrapolating from past events. *Don't let the present duplicate the past.*	
	Contextual Unpredictability Definition: Change behavior or state in ways that are determined randomly or by complex functions. Informal description: *Keep the adversary from extrapolating from similar events.* *Don't let the adversary take advantage of consistency.*	**CSA-02**

Appendix B Relationships between Cyber Resiliency Constructs

The tables in this appendix are adapted from Appendix D of NIST SP 800-160 Vol. 2 R1. They describe the relationships between cyber resiliency constructs. See Appendix D of [6] for a more complete description of the relationships and for guidance.

Table 15. Strategic Design Principles Drive Structural Design Principles

	STRATEGIC DESIGN PRINCIPLES				
STRUCTURAL DESIGN PRINCIPLES	**Focus on common critical assets**	**Support agility and architect for adaptability**	**Reduce attack surfaces**	**Assume compromised resources**	**Expect adversaries to evolve**
Limit the need for trust.			X	X	
Control visibility and use.	X		X	X	
Contain and exclude behaviors.	X			X	X
Layer defenses and partition resources.	X			X	
Plan and manage diversity.	X	X		X	
Maintain redundancy.	X	X		X	
Make resources location-versatile.	X	X			X
Leverage health and status data.	X	X		X	X
Maintain situational awareness.	X				X
Manage resources (risk-) adaptively.	X	X			X
Maximize transience.			X	X	X
Determine ongoing trustworthiness.	X			X	X
Change or disrupt the attack surface.			X	X	X
Make the effects of deception and unpredictability user-transparent.		X	X		

Table 16. Structural Design Principles and Cyber Resiliency Techniques

STRUCTURAL DESIGN PRINCIPLE	REQUIRED TECHNIQUES	OTHER TECHNIQUES
Limit the need for trust.	Privilege Restriction, Realignment	Coordinated Protection, Substantiated Integrity
Control visibility and use.	Privilege Restriction, Segmentation	Deception, Non-Persistence
Contain and exclude behaviors.	Privilege Restriction, Segmentation	Analytic Monitoring, Diversity, Non-Persistence, Substantiated Integrity
Layer defenses and partition resources.	Coordinated Protection, Segmentation	Analytic Monitoring, Diversity, Dynamic Positioning, Redundancy
Plan and manage diversity.	Diversity	Coordinated Protection, Redundancy
Maintain redundancy.	Redundancy	Coordinated Protection, Diversity, Realignment
Make resources location-versatile.	Dynamic Positioning	Adaptive Response, Diversity, Non-Persistence, Redundancy, Unpredictability
Leverage health and status data.	Analytic Monitoring, Contextual Awareness	Substantiated Integrity
Maintain situational awareness.	Contextual Awareness	Analytic Monitoring
Manage resources (risk-) adaptively.	Adaptive Response	Coordinated Protection, Deception, Dynamic Positioning, Non-Persistence, Privilege Restriction, Realignment, Redundancy, Segmentation, Unpredictability
Maximize transience.	Non-Persistence	Analytic Monitoring, Dynamic Positioning, Substantiated Integrity, Unpredictability
Determine ongoing trustworthiness.	Substantiated Integrity	Coordinated Protection
Change or disrupt the attack surface.	Dynamic Positioning, Non-Persistence	Adaptive Response, Deception, Diversity, Unpredictability
Make the effects of deception and unpredictability user-transparent.	Coordinated Protection	Adaptive Response, Deception, Unpredictability

Appendix C Cyber Resiliency Controls

Table 17 is based on Table E-1 from NIST SP 800-160 Vol. 2 R1. The rightmost column indicates the CSAs directly supported by each control, as determined by the analysis method described in Section 2.

Table 17. Cyber Resiliency Controls

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	CSAs Supported (if any)
AC-2(6)	ACCOUNT MANAGEMENT | DYNAMIC PRIVILEGE MANAGEMENT	Privilege Restriction [Dynamic Privileges] Adaptive Response [Dynamic Reconfiguration]	CSA-01, CSA-03, CSA-05, CSA-08, CSA-10
AC-2(8)	ACCOUNT MANAGEMENT | DYNAMIC ACCOUNT MANAGEMENT	Adaptive Response [Dynamic Resource Allocation, Dynamic Reconfiguration, Adaptive Management] Privilege Restriction [Dynamic Privileges]	CSA-01, CSA-03, CSA-05, CSA-08, CSA-10
AC-2(12)	ACCOUNT MANAGEMENT | ACCOUNT MONITORING FOR ATYPICAL USAGE	Analytic Monitoring [Monitoring and Damage Assessment] Substantiated Integrity [Behavior Validation]	CSA-01, CSA-07, CSA-08, CSA-10
AC-3(2)	ACCESS ENFORCEMENT | DUAL AUTHORIZATION	Privilege Restriction [Trust-Based Privilege Management]	CSA-01, CSA-03, CSA-06, CSA-10
AC-3(7)	ACCESS ENFORCEMENT | ROLE-BASED ACCESS CONTROL	Privilege Restriction [Attribute-Based Usage Restriction]	
AC-3(11)	ACCESS ENFORCEMENT | RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES	Privilege Restriction [Attribute-Based Usage Restriction]	CSA-01, CSA-03, CSA-04, CSA-08
AC-3(12)	ACCESS ENFORCEMENT | ASSERT AND ENFORCE APPLICATION ACCESS	Privilege Restriction [Attribute-Based Usage Restriction]	CSA-01, CSA-03, CSA-06, CSA-08, CSA-10
AC-3(13)	ACCESS ENFORCEMENT | ATTRIBUTE-BASED ACCESS CONTROL	Privilege Restriction [Attribute-Based Usage Restriction]	CSA-01, CSA-03, CSA-08, CSA-10
AC-4(2)	INFORMATION FLOW ENFORCEMENT | PROCESSING DOMAINS	Segmentation [Predefined Segmentation]	CSA-01, CSA-02, CSA-03, CSA-04, CSA-05
AC-4(3)	INFORMATION FLOW ENFORCEMENT | DYNAMIC INFORMATION FLOW CONTROL	Adaptive Response [Dynamic Reconfiguration, Adaptive Management]	CSA-05, CSA-08, CSA-09, CSA-10
AC-4(8)	INFORMATION FLOW ENFORCEMENT | SECURITY AND PRIVACY POLICY FILTERS	Substantiated Integrity [Integrity Checks]	CSA-01, CSA-04
AC-4(12)	INFORMATION FLOW ENFORCEMENT | DATA TYPE IDENTIFIERS	Substantiated Integrity [Integrity Checks]	CSA-01 CSA-04, CSA-09
AC-4(17)	INFORMATION FLOW ENFORCEMENT | DOMAIN AUTHENTICATION	Substantiated Integrity [Provenance Tracking]	CSA-09
AC-4(21)	INFORMATION FLOW ENFORCEMENT | PHYSICAL OR LOGICAL SEPARATION OF INFORMATION FLOWS	Segmentation [Predefined Segmentation]	CSA-01, CSA-02, CSA-03, CSA-04, CSA-05, CSA-06
AC-4(27)	INFORMATION FLOW ENFORCEMENT | REDUNDANT/INDEPENDENT FILTERING MECHANISMS	Diversity [Design Diversity] Redundancy [Replication]	
AC-4(29)	INFORMATION FLOW ENFORCEMENT | FILTER ORCHESTRATION ENGINES	Coordinated Protection [Orchestration]	
AC-4(30)	INFORMATION FLOW ENFORCEMENT | FILTER MECHANISMS USING MULTIPLE PROCESSES	Diversity [Design Diversity] Redundancy [Replication]	
AC-6	LEAST PRIVILEGE	Privilege Restriction [Trust-Based Privilege Management, Attribute-Based Usage Restriction]	CSA-01, CSA-03, CSA-06, CSA-08, CSA-10

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	CSAs Supported (if any)
AC-6(1)	LEAST PRIVILEGE | AUTHORIZE ACCESS TO SECURITY FUNCTIONS	Privilege Restriction [Attribute-Based Usage Restriction]	CSA-01, CSA-03, CSA-06, CSA-08, CSA-10
AC-6(2)	LEAST PRIVILEGE | NON-PRIVILEGED ACCESS FOR NONSECURITY FUNCTIONS	Privilege Restriction [Trust-Based Privilege Management] Realignment [Purposing]	CSA-01, CSA-06
AC-6(3)	LEAST PRIVILEGE | NETWORK ACCESS TO PRIVILEGED COMMANDS	Privilege Restriction [Trust-Based Privilege Management]	CSA-01, CSA-03, CSA-06
AC-6(4)	LEAST PRIVILEGE | SEPARATE PROCESSING DOMAINS	Privilege Restriction [Trust-Based Privilege Management, Attribute-Based Usage Restriction] Segmentation [Predefined Segmentation]	CSA-01, CSA-02, CSA-05, CSA-06, CSA-09
AC-6(5)	LEAST PRIVILEGE | PRIVILEGED ACCOUNTS	Privilege Restriction [Trust-Based Privilege Management]	CSA-01, CSA-03
AC-6(6)	LEAST PRIVILEGE | PRIVILEGED ACCESS BY NON-ORGANIZATIONAL USERS	Privilege Restriction [Trust-Based Privilege Management]	CSA-01, CSA-03
AC-6(7)	LEAST PRIVILEGE | REVIEW OF USER PRIVILEGES	Coordinated Protection [Consistency Analysis] Privilege Restriction [Trust-Based Privilege Management]	CSA-01
AC-6(8)	LEAST PRIVILEGE | PRIVILEGE LEVELS FOR CODE EXECUTION	Privilege Restriction [Attribute-Based Usage Restriction, Dynamic Privileges]	CSA-01, CSA-06, CSA-10
AC-6(10)	LEAST PRIVILEGE | PROHIBIT NON-PRIVILEGED USERS FROM EXECUTING PRIVILEGED FUNCTIONS	Privilege Restriction [Attribute-Based Usage Restriction, Trust-Based Privilege Management]	CSA-01, CSA-03, CSA-06, CSA-10
AC-7(4)	UNSUCCESSFUL LOGON ATTEMPTS | USE OF ALTERNATE AUTHENTICATION FACTOR	Diversity [Path Diversity]	CSA-05, CSA-08, CSA-09
AC-12	SESSION TERMINATION	Non-Persistence [Non-Persistent Services]	CSA-03
AC-23	DATA MINING PROTECTION	Analytic Monitoring [Monitoring and Damage Assessment] Privilege Restriction [Trust-Based Privilege Management, Attribute-Based Usage Restriction, Dynamic Privileges]	CSA-01, CSA-02, CSA-03, CSA-04, CSA-07
AU-5(3)	RESPONSE TO AUDIT PROCESSING FAILURES | CONFIGURABLE TRAFFIC VOLUME THRESHOLDS	Adaptive Response [Dynamic Resource Allocation, Adaptive Management]	CSA-08
AU-6	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING	Adaptive Response [Adaptive Management] Analytic Monitoring [Monitoring and Damage Assessment] Substantiated Integrity [Behavior Validation]	CSA-01, CSA-07, CSA-09
AU-6(3)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATE AUDIT REPOSITORIES	Analytic Monitoring [Sensor Fusion and Analysis]	CSA-07, CSA-09
AU-6(5)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | INTEGRATED ANALYSIS OF AUDIT RECORDS	Analytic Monitoring [Sensor Fusion and Analysis]	CSA-05, CSA-07, CSA-09
AU-6(6)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH PHYSICAL MONITORING	Analytic Monitoring [Sensor Fusion and Analysis]	CSA-05, CSA-07, CSA-09
AU-6(8)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | FULL TEXT ANALYSIS OF PRIVILEGED COMMANDS	Analytic Monitoring [Monitoring and Damage Assessment] Segmentation [Predefined Segmentation]	CSA-01, CSA-07, CSA-09
AU-6(9)	AUDIT RECORD REVIEW, ANALYSIS, AND REPORTING | CORRELATION WITH INFORMATION FROM NONTECHNICAL SOURCES	Analytic Monitoring [Sensor Fusion and Analysis]	CSA-05, CSA-07, CSA-09

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	CSAs Supported (if any)
AU-9(1)	PROTECTION OF AUDIT INFORMATION | HARDWARE WRITE-ONCE MEDIA	Substantiated Integrity [Integrity Checks]	CSA-01, CSA-04, CSA-08
AU-9(2)	PROTECTION OF AUDIT INFORMATION | STORE ON SEPARATE PHYSICAL SYSTEMS AND COMPONENTS	Segmentation [Predefined Segmentation]	CSA-01, CSA-02, CSA-04, CSA-05, CSA-08, CSA-09
AU-9(3)	PROTECTION OF AUDIT INFORMATION | CRYPTOGRAPHIC PROTECTION	Substantiated Integrity [Integrity Checks]	CSA-01, CSA-04, CSA-08
AU-9(5)	PROTECTION OF AUDIT INFORMATION | DUAL AUTHORIZATION	Privilege Restriction [Trust-Based Privilege Management]	CSA-01, CSA-03, CSA-04
AU-9(6)	PROTECTION OF AUDIT INFORMATION | READ-ONLY ACCESS	Privilege Restriction [Trust-Based Privilege Management, Attribute-Based Usage Restriction] Substantiated Integrity [Integrity Checks]	CSA-01, CSA-03, CSA-04, CSA-08, CSA-09
AU-9(7)	PROTECTION OF AUDIT INFORMATION | STORE ON COMPONENT WITH DIFFERENT OPERATING SYSTEM	Diversity [Architectural Diversity]	CSA-05, CSA-08, CSA-09
AU-10(2)	NON-REPUDIATION | VALIDATE BINDING OF INFORMATION PRODUCER IDENTITY	Substantiated Integrity [Provenance Tracking]	
AU-13	MONITORING FOR INFORMATION DISCLOSURE	Adaptive Response [Adaptive Management] Analytic Monitoring [Monitoring and Damage Assessment]	
AU-13(3)	MONITORING FOR INFORMATION DISCLOSURE | UNAUTHORIZED REPLICATION OF INFORMATION	Analytic Monitoring [Monitoring and Damage Assessment]	
AT-2(1)	AWARENESS TRAINING | PRACTICAL EXERCISES	Contextual Awareness [Dynamic Threat Awareness] Coordinated Protection [Self-Challenge]	
AT-2(3)	AWARENESS TRAINING | SOCIAL ENGINEERING AND MINING	Contextual Awareness [Dynamic Threat Awareness]	
AT-2(5)	AWARENESS TRAINING | ADVANCED PERSISTENT THREAT	Contextual Awareness [Dynamic Threat Awareness]	
AT-3(3)	ROLE-BASED TRAINING | PRACTICAL EXERCISES	Contextual Awareness [Dynamic Threat Awareness] Coordinated Protection [Self-Challenge]	
CA-7(3)	CONTINUOUS MONITORING | TREND ANALYSES	Contextual Analysis [Dynamic Resource Awareness, Dynamic Threat Awareness]	CSA-05, CSA-07
CA-7(5)	CONTINUOUS MONITORING | CONSISTENCY ANALYSIS	Coordinated Protection [Consistency Analysis]	CSA-08
CA-7(6)	CONTINUOUS MONITORING | AUTOMATION SUPPORT FOR MONITORING	Analytic Monitoring [Monitoring and Damage Assessment]	
CA-8	PENETRATION TESTING	Coordinated Protection [Self-Challenge]	CSA-06, CSA-10
CA-8(1)	PENETRATION TESTING | INDEPENDENT PENETRATION AGENT OR TEAM	Coordinated Protection [Self-Challenge]	CSA-06, CSA-10
CA-8(2)	PENETRATION TESTING | RED TEAM EXERCISES	Coordinated Protection [Self-Challenge]	CSA-06, CSA-10
CA-8(3)	PENETRATION TESTING | FACILITY PENETRATION TESTING	Coordinated Protection [Self-Challenge]	CSA-06, CSA-10
CM-2(7)	BASELINE CONFIGURATION | CONFIGURE SYSTEMS AND COMPONENTS FOR HIGH-RISK AREAS	Analytic Monitoring [Monitoring and Damage Assessment, Forensic and Behavioral Analysis] Realignment [Restriction]	CSA-06, CSA-07
CM-4(1)	IMPACT ANALYSES | SEPARATE TEST ENVIRONMENTS	Segmentation [Predefined Segmentation]	CSA-01, CSA-02, CSA-05, CSA-06
CM-5(4)	ACCESS RESTRICTIONS FOR CHANGE | DUAL AUTHORIZATION	Privilege Restriction [Trust-Based Privilege Management]	CSA-01, CSA-03, CSA-06, CSA-10

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	CSAs Supported (if any)
CM-5(5)	ACCESS RESTRICTIONS FOR CHANGE | PRIVILEGE LIMITATION FOR PRODUCTION AND OPERATION	Privilege Restriction [Trust-Based Privilege Management]	CSA-01, CSA-03, CSA-06
CM-5(6)	ACCESS RESTRICTIONS FOR CHANGE | LIMIT LIBRARY PRIVILEGES	Privilege Restriction Trust-Based Privilege Management]	CSA-01, CSA-03, CSA-06
CM-7(2)	LEAST FUNCTIONALITY | PREVENT PROGRAM EXECUTION	Realignment [Restriction]	CSA-06
CM-7(4)	LEAST FUNCTIONALITY | UNAUTHORIZED SOFTWARE	Realignment [Purposing]	CSA-06
CM-7(5)	LEAST FUNCTIONALITY | AUTHORIZED SOFTWARE	Privilege Restriction [Trust-Based Privilege Management] Realignment [Purposing]	CSA-01, CSA-05, CSA-06
CM-7(6)	LEAST FUNCTIONALITY | CONFINED ENVIRONMENTS WITH LIMITED PRIVILEGES	Privilege Restriction [Trust-Based Privilege Management] Segmentation [Predefined Segmentation, Dynamic Segmentation and Isolation]	CSA-06
CM-7(7)	LEAST FUNCTIONALITY | CODE EXECUTION IN PROTECTED ENVIRONMENTS	Segmentation [Predefined Segmentation]	
CM-8(3)	SYSTEM COMPONENT INVENTORY | AUTOMATED UNAUTHORIZED COMPONENT DETECTION	Analytic Monitoring [Monitoring and Damage Assessment]	CSA-07, CSA-08, CSA-09
CM-14	SIGNED COMPONENTS	Substantiated Integrity [Integrity Checks, Provenance Tracking]	CSA-01, CSA-06, CSA-09, CSA-10
CP-2(1)	CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS	Coordinated Protection [Consistency Analysis]	
CP-2(5)	CONTINGENCY PLAN | CONTINUE MISSIONS AND BUSINESS FUNCTIONS	Coordinated Protection [Orchestration] Adaptive Response [Dynamic Reconfiguration, Adaptive Management]	CSA-05, CSA-08, CSA-09, CSA-10
CP-2(8)	CONTINGENCY PLAN | IDENTIFY CRITICAL ASSETS	Contextual Awareness [Mission Dependency and Status Visualization]	CSA-05, CSA-07, CSA-08, CSA-10
CP-4(5)	SELF-CHALLENGE	Coordinated Protection [Self-Challenge]	CSA-06, CSA-08, CSA-10
CP-8(3)	TELECOMMUNICATIONS SERVICES | SEPARATION OF PRIMARY AND ALTERNATE PROVIDERS	Diversity [Architectural Diversity]	CSA-05, CSA-08, CSA-10
CP-9	SYSTEM BACKUP	Redundancy [Protected Backup and Restore]	CSA-05, CSA-08. CSA-09
CP-9(1)	SYSTEM BACKUP | TESTING FOR RELIABILITY AND INTEGRITY	Coordinated Protection [Self-Challenge] Redundancy [Protected Backup and Restore] Substantiated Integrity [Integrity Checks]	
CP-9(6)	SYSTEM BACKUP | REDUNDANT SECONDARY SYSTEM	Redundancy [Replication]	CSA-05, CSA-08, CSA-09
CP-9(7)	SYSTEM BACKUP | DUAL AUTHORIZATION	Privilege Restriction [Trust-Based Privilege Management]	CSA-01, CSA-03, CSA-06, CSA-10
CP-9(8)	SYSTEM BACKUP | CRYPTOGRAPHIC PROTECTION	Deception [Obfuscation] Redundancy [Protected Backup and Restore] Substantiated Integrity [Integrity Checks]	CSA-02, CSA-04, CSA-05, CSA-08, CSA-09
CP-11	ALTERNATE COMMUNICATIONS PROTOCOLS	Diversity [Architectural Diversity, Design Diversity]	CSA-05, CSA-08, CSA-09, CSA-10
CP-12	SAFE MODE	Adaptive Response [Adaptive Management] Realignment [Restriction]	CSA-05, CSA-08, CSA-09, CSA-10
CP-13	ALTERNATIVE SECURITY MECHANISMS	Diversity [Architectural Diversity, Design Diversity] Adaptive Response [Adaptive Management]	CSA-05, CSA-08, CSA-09, CSA-10

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	CSAs Supported (if any)
IA-2(6)	IDENTIFICATION AND AUTHENTICATION | ACCESS TO ACCOUNTS - SEPARATE DEVICE	Diversity [Path Diversity] Coordinated Protection [Calibrated Defense-in-Depth, Orchestration]	CSA-03, CSA-05
IA-2(13)	IDENTIFICATION AND AUTHENTICATION | OUT-OF-BAND AUTHENTICATION	Diversity [Path Diversity] Coordinated Protection [Calibrated Defense-in-Depth, Orchestration] Segmentation [Predefined Segmentation]	CSA-01, CSA-03, CSA-05, CSA-08
IA-3(1)	DEVICE IDENTIFICATION AND AUTHENTICATION | CRYPTOGRAPHIC BIDIRECTIONAL AUTHENTICATION	Deception [Obfuscation] Substantiated Integrity [Integrity Checks]	CSA-01, CSA-03, CSA-06
IA-10	ADAPTIVE AUTHENTICATION	Adaptive Response [Adaptive Management] Privilege Restriction [Dynamic Privileges] Coordinated Protection [Calibrated Defense-in-Depth]	CSA-01, CSA-05, CSA-06, CSA-08, CSA-09, CSA-10
IR-4(2)	INCIDENT HANDLING | DYNAMIC RECONFIGURATION	Adaptive Response [Dynamic Reconfiguration] Dynamic Positioning [Functional Relocation of Sensors]	CSA-02, CSA-05, CSA-08, CSA-09, CSA-10
IR-4(3)	INCIDENT HANDLING | CONTINUITY OF OPERATIONS	Adaptive Response [Dynamic Reconfiguration, Adaptive Management] Coordinated Protection [Orchestration]	CSA-05, CSA-08, CSA-09, CSA-10
IR-4(4)	INCIDENT HANDLING | INFORMATION CORRELATION	Coordinated Protection [Orchestration] Analytic Monitoring [Sensor Fusion and Analysis] Contextual Awareness [Dynamic Threat Awareness]	CSA-05, CSA-07, CSA-08
IR-4(9)	INCIDENT HANDLING | DYNAMIC RESPONSE CAPABILITY	Adaptive Response [Dynamic Reconfiguration]	CSA-05, CSA-08, CSA-09, CSA-10
IR-4(10)	INCIDENT HANDLING | SUPPLY CHAIN COORDINATION	Coordinated Protection [Orchestration]	CSA-10
IR-4(11)	INCIDENT HANDLING | INTEGRATED INCIDENT RESPONSE TEAM	Adaptive Response [Dynamic Reconfiguration, Adaptive Management] Analytic Monitoring [Forensic and Behavioral Analysis] Coordinated Protection [Orchestration]	CSA-05, CSA-07, CSA-08, CSA-09, CSA-10
IR-4(12)	INCIDENT HANDLING | MALICIOUS CODE AND FORENSIC ANALYSIS	Analytic Monitoring [Forensic and Behavioral Analysis] Segmentation [Predefined Segmentation]	CSA-01, CSA-07, CSA-08, CSA-09, CSA-10
IR-4(13)	INCIDENT HANDLING | BEHAVIOR ANALYSIS	Analytic Monitoring [Monitoring and Damage Assessment] Substantiated Integrity [Behavior Validation]	CSA-01, CSA-07, CSA-08
IR-5	INCIDENT MONITORING	Analytic Monitoring [Monitoring and Damage Assessment, Forensic and Behavioral Analysis]	CSA-07, CSA-08, CSA-09
MA-4(4)	NONLOCAL MAINTENANCE | AUTHENTICATION AND SEPARATION OF MAINTENANCE SESSIONS	Segmentation [Predefined Segmentation]	CSA-01, CSA-03, CSA-05
PE-3(5)	PHYSICAL ACCESS CONTROL | TAMPER PROTECTION	Substantiated Integrity [Integrity Checks]	CSA-01, CSA-03, CSA-06
PE-6	MONITORING PHYSICAL ACCESS	Analytic Monitoring [Monitoring and Damage Assessment]	CSA-07, CSA-08
PE-6(2)	MONITORING PHYSICAL ACCESS | AUTOMATED INTRUSION RECOGNITION AND RESPONSES	Analytic Monitoring [Monitoring and Damage Assessment] Adaptive Response [Adaptive Management] Coordinated Protection [Orchestration]	CSA-03, CSA-07, CSA-08, CSA-09, CSA-10

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	CSAs Supported (if any)
PE-6(4)	MONITORING PHYSICAL ACCESS | MONITORING PHYSICAL ACCESS TO SYSTEMS	Analytic Monitoring [Monitoring and Damage Assessment] Coordinated Protection [Calibrated Defense-in-Depth]	CSA-07, CSA-08
PE-9(1)	POWER EQUIPMENT AND CABLING | REDUNDANT CABLING	Redundancy [Replication]	CSA-03, CSA-05, CSA-08, CSA-09
PE-11(1)	EMERGENCY POWER | ALTERNATE POWER SUPPLY - MINIMAL OPERATIONAL CAPABILITY	Redundancy [Replication]	CSA-05, CSA-08, CSA-09
PE-11(2)	EMERGENCY POWER | ALTERNATE POWER SUPPLY - SELF-CONTAINED	Redundancy [Replication]	CSA-05, CSA-08, CSA-09
PE-17	ALTERNATE WORK SITE	Redundancy [Replication]	CSA-05, CSA-08, CSA-09
PL-8(1)	SECURITY AND PRIVACY ARCHITECTURE | DEFENSE IN DEPTH	Coordinated Protection [Calibrated Defense-in-Depth]	CSA-05, CSA-06, CSA-08
PL-8(2)	SECURITY AND PRIVACY ARCHITECTURE | SUPPLIER DIVERSITY	Diversity [Supply Chain Diversity]	CSA-08
PM-7(1)	ENTERPRISE ARCHITECTURE | OFFLOADING	Realignment [Offloading]	CSA-05, CSA-06
PM-16	THREAT AWARENESS PROGRAM	Contextual Awareness [Dynamic Threat Awareness]	CSA-07, CSA-09, CSA-10
PM-16(1)	THREAT AWARENESS PROGRAM | AUTOMATED MEANS FOR SHARING THREAT INTELLIGENCE	Contextual Awareness [Dynamic Threat Awareness]	CSA-05, CSA-07, CSA-09
PM-30(1)	SUPPLY CHAIN RISK MANAGEMENT | SUPPLIERS OF CRITICAL OR MISSION-ESSENTIAL ITEMS	Substantiated Integrity [Provenance Tracking]	
PM-31	CONTINUOUS MONITORING STRATEGY	Analytic Monitoring [Monitoring and Damage Assessment, Sensor Fusion and Analysis]	CSA-07, CSA-08, CSA-09, CSA-10
PM-32	PURPOSING	Realignment [Purposing]	CSA-06
RA-3(2)	RISK ASSESSMENT | USE OF ALL-SOURCE INTELLIGENCE	Contextual Awareness [Dynamic Threat Awareness]	
RA-3(3)	RISK ASSESSMENT | DYNAMIC THREAT AWARENESS	Contextual Awareness [Dynamic Threat Awareness] Adaptive Response [Adaptive Management]	CSA-05, CSA-07, CSA-08, CSA-10
RA-3(4)	RISK ASSESSMENT | PREDICTIVE CYBER ANALYTICS	Contextual Awareness [Dynamic Threat Awareness]	
RA-5(4)	VULNERABILITY MONITORING AND SCANNING | DISCOVERABLE INFORMATION	Analytic Monitoring [Monitoring and Damage Assessment]	
RA-5(5)	VULNERABILITY MONITORING AND SCANNING | PRIVILEGED ACCESS	Analytic Monitoring [Monitoring and Damage Assessment] Privilege Restriction [Attribute-Based Usage Restriction]	CSA-01, CSA-03, CSA-06, CSA-07, CSA-10
RA-5(6)	VULNERABILITY MONITORING AND SCANNING | AUTOMATED TREND ANALYSES	Analytic Monitoring [Sensor Fusion and Analysis]	CSA-07
RA-5(8)	VULNERABILITY MONITORING AND SCANNING | REVIEW HISTORIC AUDIT LOGS	Analytic Monitoring [Sensor Fusion and Analysis]	CSA-07, CSA-09
RA-5(10)	VULNERABILITY MONITORING AND SCANNING | CORRELATE SCANNING INFORMATION	Analytic Monitoring [Sensor Fusion and Analysis]	CSA-05, CSA-07, CSA-08

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	CSAs Supported (if any)
RA-9	CRITICALITY ANALYSIS	Contextual Awareness [Mission Dependency and Status Visualization] Realignment [Offloading]	CSA-05, CSA-07, CSA-08, CSA-10
RA-10	THREAT HUNTING	Analytic Monitoring [Monitoring and Damage Assessment] Contextual Awareness [Dynamic Threat Awareness]	CSA-05, CSA-07, CSA-08, CSA-10
SA-3(2)	SYSTEM DEVELOPMENT LIFECYCLE | USE OF LIVE OR OPERATIONAL DATA	Segmentation [Predefined Segmentation]	
SA-8(2)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | LEAST COMMON MECHANISM	Realignment [Offloading, Restriction]	
SA-8(3)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | MODULARITY AND LAYERING	Coordinated Protection [Calibrated Defense-in-Depth] Realignment [Specialization] Segmentation [Predefined Segmentation]	
SA-8(4)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | PARTIALLY ORDERED DEPENDENCIES	Coordinated Protection [Consistency Analysis]	
SA-8(7)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | REDUCED COMPLEXITY	Realignment [Purposing, Specialization]	
SA-8(8)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE EVOLVABILITY	Coordinated Protection [Orchestration] Realignment [Evolvability]	
SA-8(13)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | MINIMIZED SECURITY ELEMENTS	Realignment [Purposing, Restriction]	
SA-8(16)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SELF-RELIANT TRUSTWORTHINESS	Adaptive Response [Adaptive Management] Segmentation [Dynamic Segmentation and Isolation] Substantiated Integrity [Integrity Checks]	
SA-8(17)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE DISTRIBUTED COMPOSITION	Dynamic Positioning [Distributed Functionality]	
SA-8(18)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | TRUSTED COMMUNICATIONS CHANNELS	Privilege Restriction [Attribute-Based Usage Restriction]	
SA-8(19)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | CONTINUOUS PROTECTION	Redundancy [Protected Backup and Restore] Substantiated Integrity [Integrity Checks]	
SA-8(31)	SECURITY AND PRIVACY ENGINEERING PRINCIPLES | SECURE SYSTEM MODIFICATION	Realignment [Evolvability]	
SA-9(7)	EXTERNAL SYSTEM SERVICES | ORGANIZATION-CONTROLLED INTEGRITY CHECKING	Substantiated Integrity [Integrity Checks]	
SA-11(2)	DEVELOPER TESTING AND EVALUATION | THREAT MODELING AND VULNERABILITY ANALYSIS	Contextual Awareness [Dynamic Threat Awareness]	CSA-07
SA-11(5)	DEVELOPER TESTING AND EVALUATION | PENETRATION TESTING	Coordinated Protection [Self-Challenge]	CSA-06
SA-11(6)	DEVELOPER TESTING AND EVALUATION | ATTACK SURFACE REVIEWS	Realignment [Replacement]	CSA-06
SA-15(5)	DEVELOPMENT PROCESS, STANDARDS, AND TOOLS | ATTACK SURFACE REDUCTION	Realignment [Replacement]	CSA-06
SA-17(6)	DEVELOPER SECURITY ARCHITECTURE AND DESIGN | STRUCTURE FOR TESTING	Realignment [Evolvability]	

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	CSAs Supported (if any)
SA-17(8)	DEVELOPER SECURITY ARCHITECTURE AND DESIGN | ORCHESTRATION	Coordinated Protection [Orchestration]	CSA-05, CSA-09
SA-17(9)	DEVELOPER SECURITY ARCHITECTURE AND DESIGN | DESIGN DIVERSITY	Diversity [Design Diversity]	CSA-05, CSA-08
SA-20	CUSTOMIZED DEVELOPMENT OF CRITICAL COMPONENTS	Realignment [Specialization]	CSA-06
SA-23	SPECIALIZATION	Realignment [Specialization]	CSA-06
SC-2	SEPARATION OF SYSTEM AND USER FUNCTIONALITY	Segmentation [Predefined Segmentation]	CSA-01, CSA-02, CSA-05, CSA-06
SC-2(1)	SEPARATION OF SYSTEM AND USER FUNCTIONALITY | INTERFACES FOR NON-PRIVILEGED USERS	Segmentation [Predefined Segmentation]	CSA-01, CSA-05, CSA-06
SC-3	SECURITY FUNCTION ISOLATION	Segmentation [Predefined Segmentation]	CSA-01, CSA-02, CSA-05, CSA-06, CSA-09
SC-3(1)	SECURITY FUNCTION ISOLATION | HARDWARE SEPARATION	Segmentation [Predefined Segmentation]	CSA-01, CSA-02, CSA-05, CSA-06
SC-3(2)	SECURITY FUNCTION ISOLATION | ACCESS AND FLOW CONTROL FUNCTIONS	Segmentation [Predefined Segmentation]	CSA-01, CSA-02, CSA-03, CSA-05, CSA-06, CSA-09
SC-3(3)	SECURITY FUNCTION ISOLATION | MINIMIZE NONSECURITY FUNCTIONALITY	Realignment [Restriction]	CSA-05, CSA-06
SC-3(5)	SECURITY FUNCTION ISOLATION | LAYERED STRUCTURES	Coordinated Protection [Orchestration] Segmentation [Predefined Segmentation] Realignment [Offloading]	CSA-01, CSA-02, CSA-05, CSA-06
SC-5(2)	DENIAL-OF-SERVICE PROTECTION | CAPACITY, BANDWIDTH, AND REDUNDANCY	Adaptive Response [Dynamic Resource Allocation] Redundancy [Surplus Capacity]	CSA-03, CSA-05, CSA-08, CSA-09, CSA-10
SC-5(3)	DENIAL-OF-SERVICE PROTECTION | DETECTION AND MONITORING	Analytic Monitoring [Monitoring and Damage Assessment]	CSA-07, CSA-08
SC-7	BOUNDARY PROTECTION	Segmentation [Predefined Segmentation]	CSA-01, CSA-02, CSA-03, CSA-05, CSA-06, CSA-08, CSA-09, CSA-10
SC-7(10)	BOUNDARY PROTECTION | PREVENT EXFILTRATION	Analytic Monitoring [Monitoring and Damage Assessment] Non-Persistence [Non-Persistent Information, Non-Persistent Connectivity] Coordinated Protection [Self-Challenge]	CSA-03, CSA-04, CSA-05, CSA-09
SC-7(11)	BOUNDARY PROTECTION | RESTRICT INCOMING COMMUNICATIONS TRAFFIC	Substantiated Integrity [Provenance Tracking]	CSA-03, CSA-06
SC-7(13)	BOUNDARY PROTECTION | ISOLATION OF SECURITY TOOLS, MECHANISMS, AND SUPPORT COMPONENTS	Segmentation [Predefined Segmentation]	CSA-01, CSA-02, CSA-05, CSA-06, CSA-08, CSA-09, CSA-10
SC-7(15)	BOUNDARY PROTECTION | NETWORK PRIVILEGE ACCESSES	Realignment [Offloading] Segmentation [Predefined Segmentation] Privilege Restriction [Trust-Based Privileged Management]	CSA-01, CSA-02, CSA-03, CSA-05, CSA-06
SC-7(16)	BOUNDARY PROTECTION | PREVENT DISCOVERY OF COMPONENTS AND DEVICES	Deception [Obfuscation] Dynamic Positioning {Functional Relocation of Cyber Resources]	CSA-02, CSA-03, CSA-05
SC-7(20)	BOUNDARY PROTECTION | DYNAMIC ISOLATION AND SEGREGATION	Segmentation [Dynamic Segmentation and Isolation] Adaptive Response [Dynamic Reconfiguration]	CSA-01, CSA-02, CSA-05, CSA-06, CSA-08, CSA-09, CSA-10

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	CSAs Supported (if any)
SC-7(21)	BOUNDARY PROTECTION | ISOLATION OF SYSTEM COMPONENTS	Segmentation [Predefined Segmentation]	CSA-01, CSA-02, CSA-05, CSA-06, CSA-08, CSA-10
SC-7(22)	BOUNDARY PROTECTION | SEPARATE SUBNETS FOR CONNECTING TO DIFFERENT SECURITY DOMAINS	Segmentation [Predefined Segmentation]	CSA-01, CSA-02, CSA-05, CSA-06, CSA-08, CSA-09, CSA-10
SC-7(29)	BOUNDARY PROTECTION | SEPARATE SUBNETS TO ISOLATE FUNCTIONS	Segmentation [Predefined Segmentation]	
SC-8(1)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CRYPTOGRAPHIC PROTECTION	Deception [Obfuscation] Substantiated Integrity [Integrity Checks]	CSA-01, CSA-03, CSA-04, CSA-06
SC-8(4)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY | CONCEAL OR RANDOMIZE COMMUNICATIONS	Deception [Obfuscation] Unpredictability [Contextual Unpredictability]	CSA-02, CSA-03, CSA-04
SC-8(5)	TRANSMISSION CONFIDENTIALITY AND INTEGRITY | PROTECTED DISTRIBUTION SYSTEM	Substantiated Integrity [Integrity Checks] Segmentation [Predefined Segmentation]	CSA-01, CSA-03, CSA-04, CSA-06
SC-10	NETWORK DISCONNECT	Non-Persistence [Non-Persistent Connectivity]	CSA-02, CSA-03, CSA-05, CSA-06
SC-11	TRUSTED PATH	Segmentation [Predefined Segmentation] Substantiated Integrity [Provenance Tracking]	CSA-01, CSA-03, CSA-05, CSA-06
SC-15(1)	COLLABORATIVE COMPUTING DEVICES | PHYSICAL OR LOGICAL DISCONNECT	Non-Persistence [Non-Persistent Connectivity]	CSA-02, CSA-03, CSA-05, CSA-06
SC-16(1)	TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES | INTEGRITY VERIFICATION	Substantiated Integrity [Integrity Checks]	
SC-16(3)	TRANSMISSION OF SECURITY AND PRIVACY ATTRIBUTES | CRYPTOGRAPHIC BINDING	Substantiated Integrity [Integrity Checks]	
SC-18(5)	MOBILE CODE | ALLOW EXECUTION ONLY IN CONFINED ENVIRONMENTS	Segmentation [Dynamic Segmentation and Isolation]	CSA-01, CSA-02, CSA-05, CSA-06, CSA-10
SC-22	ARCHITECTURE AND PROVISIONING FOR NAME/ADDRESS RESOLUTION SERVICE	Redundancy [Replication]	CSA-09
SC-23(3)	SESSION AUTHENTICITY | UNIQUE SYSTEM-GENERATED SESSION IDENTIFIERS	Non-Persistence [Non-Persistent Information] Unpredictability [Temporal Unpredictability]	CSA-06
SC-25	THIN NODES	Realignment [Offloading, Restriction] Non-Persistence [Non-Persistent Services, Non-Persistent Information]	CSA-02, CSA-04, CSA-05, CSA-06
SC-26	DECOYS	Deception [Misdirection] Analytic Monitoring [Monitoring and Damage Assessment, Forensic and Behavioral Analysis]	CSA-06, CSA-07, CSA-08, CSA-09, CSA-10
SC-27	PLATFORM-INDEPENDENT APPLICATIONS	Diversity [Architectural Diversity] Realignment [Evolvability]	
SC-28(1)	PROTECTION OF INFORMATION AT REST | CRYPTOGRAPHIC PROTECTION	Deception [Obfuscation] Substantiated Integrity [Integrity Checks]	CSA-01, CSA-04, CSA-06, CSA-08
SC-29	HETEROGENEITY	Diversity [Architectural Diversity]	CSA-05, CSA-08, CSA-09, CSA-10
SC-29(1)	HETEROGENEITY | VIRTUALIZATION TECHNIQUES	Diversity [Architectural Diversity] Non-Persistence [Non-Persistent Services]	CSA-05, CSA-08, CSA-09, CSA-10
SC-30	CONCEALMENT AND MISDIRECTION	Deception [Obfuscation, Misdirection]	CSA-02
SC-30(2)	CONCEALMENT AND MISDIRECTION | RANDOMNESS	Unpredictability [Temporal Unpredictability, Contextual Unpredictability]	CSA-02

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	CSAs Supported (if any)
SC-30(3)	CONCEALMENT AND MISDIRECTION | CHANGE PROCESSING AND STORAGE LOCATIONS	Dynamic Positioning [Functional Relocation of Cyber Resources, Asset Mobility] Unpredictability [Temporal Unpredictability]	CSA-02, CSA-03, CSA-05, CSA-09
SC-30(4)	CONCEALMENT AND MISDIRECTION | MISLEADING INFORMATION	Deception [Disinformation]	
SC-30(5)	CONCEALMENT AND MISDIRECTION | CONCEALMENT OF SYSTEM COMPONENTS	Deception [Obfuscation]	CSA-02
SC-32	SYSTEM PARTITIONING	Segmentation [Predefined Segmentation]	CSA-01, CSA-02, CSA-05, CSA-06, CSA-08, CSA-10
SC-32(1)	SYSTEM PARTITIONING | SEPARATE PHYSICAL DOMAINS FOR PRIVILEGED FUNCTIONS	Segmentation [Predefined Segmentation, Dynamic Segmentation and Isolation]	CSA-01, CSA-02, CSA-05, CSA-06, CSA-08, CSA-10
SC-34	NON-MODIFIABLE EXECUTABLE PROGRAMS	Substantiated Integrity [Integrity Checks]	CSA-01, CSA-06, CSA-08, CSA-09
SC-34(1)	NON-MODIFIABLE EXECUTABLE PROGRAMS | NO WRITABLE STORAGE	Non-Persistence [Non-Persistent Information]	CSA-04, CSA-06
SC-34(2)	NON-MODIFIABLE EXECUTABLE PROGRAMS | INTEGRITY PROTECTION ON READ-ONLY MEDIA	Substantiated Integrity [Integrity Checks]	CSA-01, CSA-06, CSA-08, CSA-09
SC-35	EXTERNAL MALICIOUS CODE IDENTIFICATION	Analytic Monitoring [Monitoring and Damage Assessment, Forensic and Behavioral Analysis] Deception [Misdirection] Segmentation [Dynamic Segmentation and Isolation]	CSA-01, CSA-06, CSA-07, CSA-09, CSA-10
SC-36	DISTRIBUTED PROCESSING AND STORAGE	Dynamic Positioning [Distributed Functionality, Functional Relocation of Cyber Resources] Redundancy [Replication]	CSA-02, CSA-03, CSA-04, CSA-05, CSA-08, CSA-09
SC-36(1)	DISTRIBUTED PROCESSING AND STORAGE | POLLING TECHNIQUES	Adaptive Response [Adaptive Management] Substantiated Integrity [Behavior Validation]	CSA-01, CSA-08 CSA-10
SC-36(2)	DISTRIBUTED PROCESSING AND STORAGE | SYNCHRONIZATION	Coordinated Protection [Orchestration] Redundancy [Replication]	CSA-08
SC-37	OUT-OF-BAND CHANNELS	Diversity [Path Diversity]	CSA-05, CSA-08, CSA-09, CSA-10
SC-39	PROCESS ISOLATION	Segmentation [Predefined Segmentation, Dynamic Segmentation and Isolation]	CSA-01, CSA-02, CSA-05, CSA-06, CSA-08, CSA-10
SC-39(1)	PROCESS ISOLATION | HARDWARE SEPARATION	Segmentation [Predefined Segmentation, Dynamic Segmentation and Isolation]	CSA-01 CSA-02, CSA-05, CSA-06, CSA-08, CSA-10
SC-39(2)	PROCESS ISOLATION | SEPARATION EXECUTION DOMAINS PER THREAD	Segmentation [Predefined Segmentation, Dynamic Segmentation and Isolation]	CSA-01, CSA-02, CSA-05, CSA-06, CSA-08, CSA-10
SC-40(2)	WIRELESS LINK PROTECTION | REDUCE DETECTION POTENTIAL	Deception [Obfuscation]	CSA-02, CSA-03
SC-40(3)	WIRELESS LINK PROTECTION | IMITATIVE OR MANIPULATIVE COMMUNICATIONS DECEPTION	Deception [Obfuscation] Unpredictability [Temporal Unpredictability, Contextual Unpredictability]	CSA-02, CSA-03
SC-44	DETONATION CHAMBERS	Segmentation [Predefined Segmentation] Analytic Monitoring [Forensic and Behavioral Analysis] Deception [Misdirection]	CSA-01, CSA-02, CSA-05, CSA-06, CSA-07, CSA-09, CSA-10
SC-46	CROSS DOMAIN POLICY ENFORCEMENT	Segmentation [Predefined Segmentation]	
SC-47	ALTERNATE COMMUNICATION PATHS	Diversity [Path Diversity]	CSA-05, CSA-08, CSA-09, CSA-10

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	CSAs Supported (if any)
SC-48	SENSOR RELOCATION	Dynamic Positioning [Functional Relocation of Sensors]	CSA-09
SC-48(1)	SENSOR RELOCATION | DYNAMIC RELOCATION OF SENSORS OR MONITORING CAPABILITIES	Dynamic Positioning [Functional Relocation of Sensors]	CSA-09
SC-49	HARDWARE-ENFORCED SEPARATION AND POLICY ENFORCEMENT	Segmentation [Predefined Segmentation]	CSA-01, CSA-02, CSA-05, CSA-06, CSA-08, CSA-10
SC-50	SOFTWARE-ENFORCED SEPARATION AND POLICY ENFORCEMENT	Segmentation [Predefined Segmentation]	CSA-01, CSA-02, CSA-05, CSA-06, CSA-08, CSA-10
SC-51	HARDWARE-BASED PROTECTION	Substantiated Integrity [Integrity Checks]	CSA-01, CSA-06, CSA-08
SI-3(10)	MALICIOUS CODE PROTECTION | MALICIOUS CODE ANALYSIS	Analytic Monitoring [Forensic and Behavioral Analysis]	CSA-07, CSA-08, CSA-09, CSA-10
SI-4(1)	SYSTEM MONITORING | SYSTEM-WIDE INTRUSION DETECTION SYSTEM	Analytic Monitoring [Sensor Fusion and Analysis] Contextual Awareness [Mission Dependency and Status Visualization]	CSA-05, CSA-07, CSA-08, CSA-09, CSA-10
SI-4(2)	SYSTEM MONITORING | AUTOMATED TOOLS AND MECHANISMS FOR REAL-TIME ANALYSIS	Analytic Monitoring [Monitoring and Damage Assessment] Contextual Awareness [Mission Dependency and Status Visualization] Substantiated Integrity [Behavior Validation]	CSA-01, CSA-03, CSA-05, CSA-07, CSA-08, CSA-09, CSA-10
SI-4(3)	SYSTEM MONITORING | AUTOMATED TOOL AND MECHANISM INTEGRATION	Analytic Monitoring [Sensor Fusion and Analysis] Adaptive Response [Adaptive Management]	CSA-05, CSA-07, CSA-08, CSA-10
SI-4(4)	SYSTEM MONITORING | INBOUND AND OUTBOUND COMMUNICATIONS TRAFFIC	Analytic Monitoring [Monitoring and Damage Assessment] Substantiated Integrity [Behavior Validation]	CSA-01, CSA-03, CSA-07, CSA-08, CSA-09, CSA-10
SI-4(7)	SYSTEM MONITORING | AUTOMATED RESPONSE TO SUSPICIOUS EVENTS	Analytic Monitoring [Monitoring and Damage Assessment] Adaptive Response [Adaptive Management]	CSA-05, CSA-06, CSA-07, CSA-08, CSA-09, CSA-10
SI-4(10)	SYSTEM MONITORING | VISIBILITY OF ENCRYPTED COMMUNICATIONS	Analytic Monitoring [Monitoring and Damage Assessment]	CSA-07
SI-4(11)	SYSTEM MONITORING | ANALYZE COMMUNICATIONS TRAFFIC ANOMALIES	Analytic Monitoring [Monitoring and Damage Assessment]	CSA-07, CSA-08, CSA-10
SI-4(13)	SYSTEM MONITORING | ANALYZE TRAFFIC AND EVENT PATTERNS	Analytic Monitoring [Monitoring and Damage Assessment] Substantiated Integrity [Behavior Validation]	CSA-01, CSA-03, CSA-07, CSA-08, CSA-09, CSA-10
SI-4(16)	SYSTEM MONITORING | CORRELATE MONITORING INFORMATION	Analytic Monitoring [Sensor Fusion and Analysis] Contextual Awareness [Dynamic Resource Awareness]	CSA-07, CSA-08
SI-4(17)	SYSTEM MONITORING | INTEGRATED SITUATIONAL AWARENESS	Analytic Monitoring [Sensor Fusion and Analysis] Contextual Awareness [Dynamic Resource Awareness]	CSA-07, CSA-08, CSA-09
SI-4(18)	SYSTEM MONITORING | ANALYZE TRAFFIC AND COVERT EXFILTRATION	Analytic Monitoring [Monitoring and Damage Assessment]	CSA-07, CSA-08, CSA-09, CSA-10
SI-4(24)	SYSTEM MONITORING | INDICATORS OF COMPROMISE	Analytic Monitoring [Monitoring and Damage Assessment, Sensor Fusion and Analysis]	CSA-05, CSA-07, CSA-08, CSA-09, CSA-10
SI-4(25)	SYSTEM MONITORING | OPTIMIZE NETWORK TRAFFIC ANALYSIS	Analytic Monitoring [Monitoring and Damage Assessment, Sensor Fusion and Analysis]	CSA-07
SI-6	SECURITY AND PRIVACY FUNCTION VERIFICATION	Substantiated Integrity [Integrity Checks]	CSA-01, CSA-06, CSA-08

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	CSAs Supported (if any)
SI-7	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY	Substantiated Integrity [Integrity Checks]	CSA-01, CSA-04, CSA-06, CSA-08, CSA-09, CSA-10
SI-7(1)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY CHECKS	Substantiated Integrity [Integrity Checks]	CSA-01, CSA-04, CSA-06, CSA-08, CSA-09
SI-7(5)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | AUTOMATED RESPONSE TO INTEGRITY VIOLATIONS	Substantiated Integrity [Integrity Checks] Adaptive Response [Adaptive Management]	CSA-01, CSA-04, CSA-05, CSA-08, CSA-09, CSA-10
SI-7(6)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CRYPTOGRAPHIC PROTECTION	Substantiated Integrity [Integrity Checks]	CSA-01, CSA-04, CSA-06, CSA-08, CSA-09
SI-7(7)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRATION OF DETECTION AND RESPONSE	Substantiated Integrity [Integrity Checks] Analytic Monitoring [Monitoring and Damage Assessment]	CSA-01, CSA-07, CSA-08, CSA-09, CSA-10
SI-7(9)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | VERIFY BOOT PROCESS	Substantiated Integrity [Integrity Checks]	CSA-01, CSA-06, CSA-08
SI-7(10)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | PROTECTION OF BOOT FIRMWARE	Substantiated Integrity [Integrity Checks]	CSA-01, CSA-06, CSA-08
SI-7(12)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | INTEGRITY VERIFICATION	Substantiated Integrity [Integrity Checks]	CSA-01, CSA-06, CSA-10
SI-7(15)	SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | CODE AUTHENTICATION	Substantiated Integrity [Provenance Tracking]	CSA-06, CSA-10
SI-10(3)	INFORMATION INPUT VALIDATION |PREDICTABLE BEHAVIOR	Substantiated Integrity [Behavior Validation]	CSA-01, CSA-06
SI-10(5)	INFORMATION INPUT VALIDATION | RESTRICT INPUTS TO TRUSTED SOURCES AND APPROVED FORMATS	Substantiated Integrity [Provenance Tracking]	CSA-03, CSA-06
SI-14	NON-PERSISTENCE	Non-Persistence [Non-Persistent Services]	CSA-02, CSA-05, CSA-06
SI-14(1)	NON-PERSISTENCE | REFRESH FROM TRUSTED SOURCES	Non-Persistence [Non-Persistent Services, Non-Persistent Information] Substantiated Integrity [Provenance Tracking]	CSA-02, CSA-04, CSA-05, CSA-06, CSA-08, CSA-09, CSA-10
SI-14(2)	NON-PERSISTENCE | NON-PERSISTENT INFORMATION	Non-Persistence [Non-Persistent Information]	CSA-04
SI-14(3)	NON-PERSISTENCE | NON-PERSISTENT CONNECTIVITY	Non-Persistence [Non-Persistent Connectivity]	CSA-02, CSA-03, CSA-05, CSA-06
SI-15	INFORMATION OUTPUT FILTERING	Substantiated Integrity [Integrity Checks]	CSA-01
SI-16	MEMORY PROTECTION	Diversity [Synthetic Diversity] Realignment [Restriction] Unpredictability [Temporal Unpredictability]	CSA-05, CSA-08
SI-19(4)	DE-IDENTIFICATION | REMOVAL, MASKING, ENCRYPTION, HASHING, OR REPLACEMENT OF DIRECT IDENTIFIERS	Deception [Obfuscation]	
SI-19(6)	DE-IDENTIFICATION | DIFFERENTIAL PRIVACY	Deception [Obfuscation] Uncertainty [Contextual Uncertainty]	
SI-19(8)	DE-IDENTIFICATION | MOTIVATED INTRUDER	Coordinated Protection [Self-Challenge]	
SI-20	TAINTING	Deception [Tainting]	
SI-21	INFORMATION REFRESH	Non-Persistence [Non-Persistent Information]	CSA-02, CSA-04

CONTROL NO.	CONTROL NAME	RESILIENCY TECHNIQUE [APPROACHES]	CSAs Supported (if any)
SI-22	INFORMATION DIVERSITY	Diversity [Information Diversity]	CSA-08
SI-23	INFORMATION FRAGMENTATION	Dynamic Positioning [Fragmentation]	CSA-02, CSA-04
SR-3(1)	SUPPLY CHAIN CONTROLS AND PROCESSES | DIVERSE SUPPLY CHAIN	Diversity [Supply Chain Diversity]	CSA-08
SR-3(2)	SUPPLY CHAIN CONTROLS AND PROCESSES | LIMITATION OF HARM	Diversity [Supply Chain Diversity] Deception [Obfuscation]	CSA-02
SR-4	PROVENANCE	Substantiated Integrity [Provenance Tracking]	CSA-06, CSA-10
SR-4(1)	PROVENANCE | IDENTITY	Substantiated Integrity [Provenance Tracking]	
SR-4(2)	PROVENANCE | TRACK AND TRACE	Substantiated Integrity [Provenance Tracking]	
SR-4(3)	PROVENANCE | VALIDATE AS GENUINE AND NOT ALTERED	Substantiated Integrity [Integrity Checks, Provenance Tracking]	CSA-01, CSA-06, CSA-10
SR-4(4)	PROVENANCE | SUPPLY CHAIN INTEGRITY – PEDIGREE	Substantiated Integrity [Provenance Tracking]	
SR-5	ACQUISITION STRATEGIES, TOOLS, AND METHODS	Substantiated Integrity [Integrity Checks, Provenance Tracking] Deception [Obfuscation]	CSA-02, CSA-10
SR-5(1)	ACQUISITION STRATEGIES, TOOLS, AND METHODS | ADEQUATE SUPPLY	Redundancy [Replication] Diversity [Supply Chain Diversity]	CSA-08
SR-6(1)	SUPPLIER ASSESSMENTS AND REVIEWS | TESTING AND ANALYSIS	Coordinated Protection [Self-Challenge] Analytic Monitoring [Monitoring and Damage Assessment]	CSA-06, CSA-07
SR-7	SUPPLY CHAIN OPERATIONS SECURITY	Deception [Obfuscation, Disinformation, Self-Challenge]	
SR-9	TAMPER RESISTANCE AND DETECTION	Substantiated Integrity [Integrity Checks]	CSA-01, CSA-03, CSA-06, CSA-09, CSA-10
SR-9(1)	TAMPER RESISTANCE AND DETECTION | MULTIPLE PHASES OF SYSTEM DEVELOPMENT LIFE CYCLE	Substantiated Integrity [Integrity Checks] Deception [Obfuscation]	CSA-01, CSA-02, CSA-06
SR-10	INSPECTION OF SYSTEMS OR COMPONENTS	Substantiated Integrity [Integrity Checks] Analytic Monitoring [Monitoring and Damage Assessment, Forensic and Behavioral Analysis]	CSA-01, CSA-06, CSA-07
SR-11	COMPONENT AUTHENTICITY	Substantiated Integrity [Integrity Checks, Provenance Tracking]	CSA-01, CSA-06
SR-11(3)	COMPONENT AUTHENTICITY | ANTI-COUNTERFEIT SCANNING	Substantiated Integrity [Integrity Checks]	

Appendix D Cyber Survivability Attributes and Cyber Resiliency Strategic and Structural Design Principles

Table 18 provides the CSA exemplar language taken from [1] [2], and identifies the cyber resiliency strategic and *structural* design principles which align with each CSA.

Table 18. CSA Exemplar Language

Pillar	CSA	Exemplar Language (Threshold and Objective Statements)	CR Strategic and *Structural* Design Principle(s)
Prevent	CSA-01: Control Access	System shall only allow identified, authenticated, and authorized persons and non-person entities (including all assigned cyber defenders and their tools) access or interconnection to system or sub-system elements. The capability shall enforce a validation mechanism to protect the C, I, A [confidentiality, integrity, and availability] of system resources (e.g., memory, files, interfaces, logical networks). The system shall employ anti-tamper measures that include features for protection of critical system components, information technologies, and maintenance of technology / program protection. Physical access to the system shall also be controlled.	Assume compromised resources. *Control visibility and use.* *Determine ongoing trustworthiness.*
	CSA-02: Reduce System's Cyber Detectability	System survivability requires that signaling and communications (both wired and wireless) implemented by the system (or state "supported by system/capability") shall minimize the ability an adversary to monitor and/or target system and/or supported DoD weapon systems through its emanations, which may include deception.	Reduce attack surfaces. *Control visibility and use.* *Maximize transience.* Support agility and architect for adaptability. *Make resources location-versatile.*
	CSA-03: Secure Transmissions and Communications	System shall ensure all transmissions and communications of data 'in transit' are protected commensurate with its confidentiality and integrity requirements. System shall only use NSA certified cryptographic capabilities.	Focus on common critical assets. *Layer defenses and partition resources.* *Maintain redundancy.* *Determine ongoing trustworthiness.* *Limit the need for trust.* *Maximize transience.* Assume compromised resources. *Change or disrupt the attack surface.* *Limit the need for trust.* *Control visibility and use.*
	CSA-04: Protect System's Information from Exploitation	System shall ensure all data 'at rest' is protected commensurate with its confidentiality and integrity requirements. System shall prevent unauthorized access, use, modification, and transfer/removal of data, including attempted exfiltration, from the system to unauthorized person and non-person entities throughout the system's lifecycle (including development).	Focus on common critical assets. *Contain and exclude behaviors.* *Layer defenses and partition resources.* *Maximize transience.* *Determine ongoing trustworthiness.* *Change or disrupt the attack surface.* *Control visibility and use.*

Pillar	CSA	Exemplar Language (Threshold and Objective Statements)	CR Strategic and *Structural* Design Principle(s)
	CSA-05: Partition and Ensure Critical Functions at Mission Completion Performance Levels	System partitioning shall implement technical / logical mitigations including logical and physical segmentation. The system shall be able to maintain mission critical functions at minimum performance thresholds identified within the system's CONOPS. Compromise of non-critical functions shall not significantly impact system mission capability.	Focus on common critical assets. *Plan and manage diversity.* *Maintain redundancy.* *Manage resources (risk-) adaptively.* *Leverage health and status data.* *Maximize transience.* Assume compromised resources. *Change or disrupt the attack surface.* *Limit the need for trust.* *Maximize transience.* *Layer defenses and partition resources.*
	CSA-06: Minimize and Harden Attack Surfaces	System shall automatically disable all unauthorized ports, protocols, and services (PPS), including access points, by default. Any deviations from PPS baselines shall be approved and documented by a configuration management board. System shall support automated monitoring and logging of system attack surface and associated cyber-events. Any removable media use must be approved, documented and strictly monitored.	Reduce attack surfaces. *Limit the need for trust.* *Change or disrupt the attack surface.* *Make the effects of deception and unpredictability user-transparent.* *Determine ongoing trustworthiness.* *Contain and exclude behaviors.* *Layer defenses and partition resources.* Expect adversaries to evolve. *Contain and exclude behaviors.* Assume compromised resources. *Leverage health and status data.*
Mitigate	CSA-07: Baseline & Monitor Systems and Detect Anomalies	System shall implement and maintain a cyber survivability configuration baseline for its GOTS/COTS HW, SW, FW and open source modules, by version number to ensure an operationally acceptable cyber risk posture 24/7 (note: drives CDRLs). System shall monitor, detect and report system health status and anomalies indicative of cyber events, based on its current adversary cyber threat intelligence, CONOPS, and Mission Relevant Terrain in Cyberspace (MRT-C). Applicable report detail shall be provided to users, system operators and assigned cyber defenders (e.g., system shall report anomalies such as configuration changes, cyber-event indicators, slowed processing or loss of functionality within T = (# of seconds/minutes) [specified by sponsor].	Focus on common critical assets. *Leverage health and status data.* *Maintain situational awareness.*
	CSA-08: Manage System Performance and Enable Cyberspace Defense	If anomalies are detected and/or cyber-events degrade system capability, the system shall be sufficiently resilient to mitigate cyber-related event effects through orderly, structured and prioritized system responses, in order to ensure minimum mission functionality requirements [system functionality threshold specified by sponsor] to complete the current mission or return for recovery. The system shall enable assigned cyber defenders to impose effects on adversaries to counter their operations and objectives. Alternatively, the mission commander shall be able to selectively disconnect/disable subsystems that are not critical as well as isolate the system from integrated platform systems and/or the Department of Defense Information Network (DoDIN).	Focus on common critical assets. *Control visibility and use.* *Contain and exclude behaviors.* *Maintain situational awareness.* *Maintain redundancy.* Support agility and architect for adaptability. *Plan and manage diversity.* *Maintain redundancy.* *Leverage health and status data.* *Manage resources (risk-) adaptively.* Expect adversaries to evolve. *Manage resources (risk-) adaptively.* *Determine ongoing trustworthiness.*

Pillar	CSA	Exemplar Language (Threshold and Objective Statements)	CR Strategic and *Structural* Design Principle(s)
Recover	CSA-09: Recover System Capabilities	After a cyber-event, the system shall be capable of being restored to a known good configuration from a trusted source; at a minimum, restored to partial mission capability, between mission cycles or within xx hours [specified by sponsor], to fight another day. System recovery shall prioritize cyber operational resiliency functions [specified by sponsor].	Support agility and architect for adaptability. *Plan and manage diversity.* *Maintain redundancy.* *Manage resources (risk-) adaptively.* Assume compromised resources. *Contain and exclude behaviors.* *Layer defenses and partition resources.* *Determine ongoing trustworthiness.* Expect adversaries to evolve. *Make resources location-versatile.* *Leverage health and status data.* *Maintain situational awareness.*
Adapt **Support DevOps – All Three Pillars**	CSA-10: Actively Manage System's Configurations to Achieve and Maintain an Operationally-relevant Cyber Risk Posture	Throughout a system's lifecycle and within one standard mission cycle of xx hours [specified by sponsor] of identification of a drop in cyber risk posture below its commensurate CSRC level, the system shall have a configuration management process, supported by automated capabilities and technology refresh options, to achieve and continuously maintain an objectively assessed and operationally-relevant risk posture. The process shall include inputs from operators, defenders and intel analysts to continuously assess changes in adversary threat, and include a machine readable Bill of Materials (BOM) of the system's GOTS/COTS HW, SW, FW and open source modules for a supply chain risk assessment prior to each milestone decision and supported release. The process shall determine the sufficiency of system cyber survivability and support a DevOps framework to prioritize vulnerability mitigation and remediation in the system and connected infrastructure with greatest mission risks. (note: drives CDRLs)	Focus on common critical assets. *Contain and exclude behaviors.* *Plan and manage diversity.* *Leverage health and status data.* *Manage resources (risk-) adaptively.* *Determine ongoing trustworthiness.* Expect adversaries to evolve. *Maintain situational awareness.*

Appendix E Abbreviations and Acronyms

Term	Definition
AFRL	Air Force Research Laboratory
ATT	Adversary Threat Tier
ATT&CK®	Adversary Tactics Techniques and Common Knowledge®
BOM	Bill of Materials
CDRL	Contract Data Requirements List
CIO	Chief Information Officer
CNSS	Committee on National Security Systems
CNSSI	CNSS Instruction
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
CSA	Cyber Survivability Attribute
CSEIG	Cyber Survivability Endorsement Implementation Guide
CSRC	Cyber Survivability Risk Category
CTI	Cyber Threat Intelligence
CTTX	Cyber Tabletop Exercise
CUI	Controlled Unclassified Information
DoD	Department of Defense
DoDIN	Department of Defense Information Network
FW	Firmware
GOTS	Government Off-the-Shelf
HW	Hardware
JCIDS	Joint Capabilities Integration and Development System
JCS	Joint Chiefs of Staff
KPP	Key Performance Parameter
MRT-C	Mission Relevant Terrain in Cyberspace
NIST	National Institute of Standards and Technology
NSA	National Security Agency
POET	Political, Operational, Economic, Technical
PPS	Ports, Protocols, and Services
RMF	Risk Management Framework

SDLC	System Development Lifecycle
SME	Subject Matter Expert
SP	[NIST] Special Publication
SS	System Survivability
SW	Software
TTPs	Tactics, Techniques, and Procedures
TTX	Tabletop Exercise